ACCS 1: 2025

Certification Scheme for Age Assurance Systems and Components

Superseded

Introduction

Age Assurance Systems utilise one or more methods (age verification, age estimation, age inference or successive validation) to provide a relying party with the necessary information to make an age-related eligibility decision. These systems are increasingly deployed in both online and offline contexts to manage access to age-restricted goods, services, venues and content.

This document, ACCS 1:2025 – *Technical Requirements for Age Assurance Systems*, consolidates and supersedes ACCS 1:2020 (Age Estimation Technologies) and ACCS 4:2020 (Age Assurance Systems), together with the 2024 Addendum on Certification Levels. It reflects the withdrawal of PAS 1296:2018 as a UK national specification and establishes alignment with ISO/IEC 27566-1:2025 – *Information security, cybersecurity and privacy protection — Age assurance systems — Part 1: Framework*, which now serves as the global benchmark for age assurance. Supporting references include IEEE 2089.1:2024 for online age verification and where relevant, the ISO/IEC 25000 (SQuaRE) product quality model and the ISO/IEC 29119 software testing series.

The Scheme has been developed as a **Type 6 certification scheme** under ISO/IEC 17067, operated in conformity with ISO/IEC 17065. Certification is based on a structured audit process that integrates system evaluation, component testing and review of practice statements. Testing activities are not offered as a standalone laboratory service but are conducted solely as part of the conformity assessment cycle to support certification decisions. Certification may therefore be applied either to complete systems or to individual components (for example, binding modules, liveness detection, identity document scanning or orchestration services), provided they are defined as targets of evaluation within the scope of this scheme.

The objectives of this scheme are to:

- Validate and certify systems and components that help prevent harm to children and mitigate nuisance or risk associated with access to age-restricted goods, content, services, venues and spaces.
- Improve the quality, consistency and performance of age assurance methods across different contexts of use.

© Age Check Certification Scheme Limited

- Provide consumers, regulators, law enforcement authorities and commercial relying parties with a trusted certification framework to identify suitable providers and components.
- Support organisations in demonstrating compliance with legal, regulatory and data protection obligations, including UK GDPR and equivalent international provisions.
- Mitigate risks of non-compliance, including criminal or civil sanctions, reputational damage and licensing or regulatory action.

Certification to ACCS 1:2025 can be conducted by any duly accredited conformity assessment body in accordance with ISO 17065.

Transition Note

ACCS 1:2025 represents the managed transition of the Age Check Certification Scheme from PAS 1296:2018 to ISO/IEC 27566-1:2025. PAS 1296 provided the initial framework for age check services but was limited in scope and jurisdiction. With its withdrawal as a British Standards Institution (BSI) specification, ISO/IEC 27566-1 provides a comprehensive, internationally recognised framework for age assurance. This standard therefore merges and replaces the technical requirements previously set out in ACCS 1:2020 and ACCS 4:2020, incorporates the 2024 Addendum on certification levels and embeds the new requirements of ISO/IEC 27566-1 and IEEE 2089.1. Certification bodies, auditors and scheme clients should regard ACCS 1:2025 as the authoritative standard for certification, with all references to PAS 1296 superseded.

The ISO/IEC 27566 family of standards is still under active development. In particular, ISO/IEC CD 27566-3 (*Age assurance systems — Part 3: Comparison or analysis*) is at the Committee Draft stage. While not yet an adopted international standard and therefore not normative to this scheme, its terminology, concepts and themes are likely to influence the evolution of global practice.

ACCS 1:2025 has been developed with awareness of these emerging directions and adopts compatible language and approaches where appropriate, in anticipation of future alignment. The Scheme Owner will review subsequent parts of ISO/IEC 27566 as they progress to publication and incorporate them into the scheme as normative references where relevant.

Superseded

Contents

Introduction 1

Transition Note 2

1. Scope 8

Scope Boundary Statement 9

2. Normative References 10

3. Terms and Definitions 11

4. Scope of the age assurance system under analysis or comparison 13

4.1 General 13

4.2 Age Assurance Providers 13

4.3 Relying Parties 13

4.4 Intermediaries 14

4.5 Declaration of Threats and Attack Vectors 14

4.6 Definition of Boundaries 14

4.7 Contexts of Use 15

4.8 Ongoing Monitoring and Change Control 15

4.8.1 Certification Cycle 15

4.8.2 Automated Continuous Monitoring 16

4.8.3 Change Management 16

4.8.4 Minor vs Major Change Parameters 16

4.8.5 Withdrawal or Suspension 16

4.9 Data Dependencies 16

4.10 Assumptions and Exclusions 17

5. Practice Statements 18

5.1 General Requirements 18

5.2 Content of Practice Statements 18

5.2.1 Core Content Requirements 18

5.2.2 Additional Content Requirements 18

5.3 Basis for Assessment 19

5.4 Updates and Maintenance 19

5.5 Structured Submission 19

5.6 Auditor Responsibilities 19

5.7 Configuration Management 19

5.8 Change Control, Documentation and Record Keeping 20

5.9 Recognition of Other Certifications and External Evidence 20

5.10 External Certification Change Notification 21

Superseded

6. Stage One Audit 22
6.1 Purpose 22
6.2 Scope of Review 22
6.3 Legal and Regulatory Requirements 22
6.4 Impartiality and Conflicts of Interest 22
6.5 Privacy and Data Protection Baseline 23
6.6 Risk Management and Attack Vectors 23
6.7 Management System Readiness 23
6.8 Monitoring and Continuous Improvement 23
6.9 Outcomes of Stage One Audit 23
7. Selection and Specification of Testing 24
7.1 Purpose 24
7.2 Competence of Test Analysts 24
7.3 Development of Test Plans 24
7.4 Test Selection 24
7.5 Sample Size and Demographics 25
7.6 Indicators of Effectiveness 25
7.7 National and Jurisdictional Requirements 25
7.8 Documentation and Records 25
7.9 Recognition of External Testing 26
7.10 Outsourced Testing to Approved Laboratories 26
7.11 Statistical Assurance Framework (Alternative Evidence Models) 26
7.12 Minimum Stratified Floors (when using reduced-N designs) 27
7.13 Acceptance Rules (examples) 27
7.14 Data Integrity & Anti-gaming Controls 27
8. Execution of Testing and Reporting of Analysis 28
8.1 Purpose 28
8.2 Execution of Testing 28
8.3 Analysis of Results 28
8.4 Reporting of Results 28
8.5 Reporting at Component Level 29
8.6 Submission to Conformity assessment body 29
9. Stage Two Audit (Specific Requirements) 29
9.1 Purpose 29
9.2 Mandatory Audit Activities 29
9.3 Evidence Requirements 30

Superseded

9.4 Conformity Assessment Criteria 30
9.5 Component and System-Level Requirements 31
9.6 Jurisdictional and Sectoral Requirements 31
9.7 Audit Findings and Reporting 31
10. Reporting of Indicators of Effectiveness 31
10.1 Purpose 31
10.2 General Requirements 31
10.3 Levels of Effectiveness 32
10.4 Statistical Basis 32
10.5 Component and System-Level Reporting 32
10.6 Demographic and Contextual Reporting 32
10.7 Local Indicators of Effectiveness 33
10.8 Reporting Format 33
11. Audit Report on Stage Two and Preparation for Evaluation Review 33
11.1 Purpose 33
11.2 General Requirements 33
11.3 Content of the Audit Report 34
11.4 Preparation for Evaluation Review 35
11.5 Reporting Format 35
12. Evaluation Review and Certification Decision 35
12.1 Purpose 35
12.2 Evaluation Review 35
12.3 Certification Decision 36
12.4 Certificate and Schedule of Certification 36
12.4.1 Certificate of Conformity 36
12.4.2 Schedule of Certification 36
12.5 Public Registry and Use of Marks 37
12.6 Optional Subsequent Certification by IEEE 37
13. Continuous Monitoring and Surveillance 38
13.1 Purpose 38
13.2 Certification Cycle 38
13.3 Surveillance Audits 38
13.4 Continuous Monitoring 38
13.5 Intervening Audits and Notifications 39
13.6 Recertification Audits 39
14. Future Alignment and Revision 39

Superseded

Annex A — Transition & Alignment from PAS 1296 and Legacy ACCS Standards 40
A.1 Purpose and use 40
A.2 What changed at a glance 40
A.3 Concept and terminology alignment 41
A.4 Requirement lineage tables 41
A.4.1 Scope, context and boundaries 41
A.4.2 Practice statements 42
A.4.3 Testing & indicators 42
A.4.4 Privacy, security, acceptability 42
A.4.5 Lifecycle control 42
A.5 Migration guidance for existing certificate holders 43
A.5.1 Who this applies to 43
A.5.2 Minimum migration steps 43
A.5.3 Timelines (default) 43
A.6 Equivalence, expansions and retirements 43
A.7 Optional interoperability and IEEE path 44
A.8 Governance and updates 44
A.9 Informative checklist (for auditors during transition) 44
Annex B — Calculation of Audit Effort 44
B.1 Purpose and scope 44
B.2 Structure of audit effort 45
B.3 Base audit effort 45
B.4 Multipliers 45
B.4.1 Component multiplier 45
B.4.2 Role multiplier 45
B.4.3 Contexts of use multiplier 46
B.4.4 Criticality multiplier 46
B.5 Reductions 46
B.6 Documentation 46
B.7 Updates 47
Annex C — Practice Statement Template 47
C.1 Purpose 47
C.2 Template structure 47
C.3 Guidance notes 49
Annex D — Stage One Audit Report Template 49
D.1 Purpose 49

Superseded

D.2 Template Structure 50
Annex E — Stage Two Audit Report Template 52
E.1 Purpose 52
E.2 Template Structure 52
Annex F — Evaluation Review Template 54
F.1 Purpose 54
F.2 Template Structure 55
Annex G — Model Certificate and Schedule of Certification 56
G.1 Purpose 56
G.3 Model Schedule of Certification 57
G.4 Public Registry Statement 58
Annex H — Normative Mapping of “Shall” Requirements 59
H.1 Method and maintenance 59
H.2 ISO/IEC 27566-1 “Shall” requirements → ACCS 1:2025 clauses 59
H.2.1 Practice statements and governance (ISO/IEC 27566-1, Clause 10) 59
H.2.2 Functional characteristics and operation 60
H.2.3 Performance and indicators 60
H.2.4 Privacy 60
H.2.5 Security (including attacks) 61
H.2.6 Lifecycle, monitoring, change control 61
H.3 IEEE 2089.1 “Shall” requirements → ACCS 1:2025 clauses 61
H.3.1 Interoperability and result exchange 61
H.3.2 Outcomes, user rights and data handling 62
H.4 Testing, reporting and indicators (cross-standard mapping) 62
H.5 Certificates, schedules and transparency 63
H.6 Gaps and handling notes 63
H.7 Auditor use 63

Superseded

1. Scope

The Age Check Certification Scheme (ACCS) Standards apply to clients submitting age assurance systems, components or services for certification and who wish to use the ACCS certification mark as a mark of conformity.

This part of the ACCS Standards:

- establishes the normative definitions applicable to age assurance systems and components, by reference to ISO/IEC 27566-1:2025 and other relevant international standards;
- identifies the system, component or service under evaluation for the purpose of assessing functional, performance, privacy, security and acceptability characteristics;
- sets out the requirements for age assurance systems and components to demonstrate conformity and fitness for deployment within their intended context of use.

Certification under this scheme may apply either to:

- **Complete age assurance systems** deployed by Age Assurance Providers or Relying Parties; or
- **Individual components** within such systems (for example, binding mechanisms, liveness detection, identity document scanning or orchestration functions), provided they can be defined as systems or components under analysis within the scope of this scheme.

These technical requirements are applicable to the following categories of scheme clients:

- **Age Assurance Providers** – entities responsible for providing age assurance results to relying parties, either directly or via applications placed under the control of individuals (e.g. applications using digital credentials).
- **Relying Parties** – entities that depend upon an age assurance result to make an age-related eligibility decision, whether in relation to goods, services, venues, spaces or online content.
- **Intermediaries** – entities that facilitate interactions between individuals, providers and relying parties or that provide supporting components, data sources or orchestration services (e.g. credential issuers, credit agencies, mobile network operators orchestration platforms).

For the purposes of this scheme, Age Assurance Providers may offer one or more of the following methods:

- **Age verification**: calculating the difference between a verified year or date of birth and a subsequent date.
- **Age estimation**: analysing biological or behavioural features that vary with age.
- **Age inference**: using verified information that indirectly implies an individual is above, below or within a defined age range.

Superseded

- **Successive validation**: applying multiple methods sequentially or in combination to strengthen the reliability of an age assurance result.

Scope Boundary Statement

This scheme applies to the certification of age assurance systems, services and components as defined in this document. Certification may be granted for:

- **Complete systems** operated by age assurance providers or relying parties; and
- **Individual components** (including methods such as verification, estimation, inference, binding, liveness detection, successive validation orchestration or delivery mechanisms), where those components can be defined as a component under analysis and tested in accordance with the scheme requirements.

The following boundaries apply:

- Certification under this scheme does **not** extend to the certification of information society services, content moderation policies or age-appropriate design features beyond their reliance on age assurance results. Such matters may fall within other ACCS Standards (e.g. ACCS 3:2021 Age-Appropriate Design).
- The scheme does not certify an organisation's **legal compliance in its entirety**; it certifies conformity of the defined system or component against the technical requirements of this scheme, which are based on ISO/IEC 27566-1 and supporting normative references.
- Testing of systems and components is conducted solely within the framework of this certification scheme and forms part of the conformity assessment cycle under ISO/IEC 17065. Testing results are not issued as stand-alone laboratory reports.

All certifications issued under this scheme are subject to **ongoing monitoring** to ensure continued conformity. This includes:

- **Automated continuous monitoring**, where feasible, to detect changes in performance, reliability or compliance indicators of deployed systems or components.
- Annual **surveillance audits**, focused on changes to practice statements, system updates and performance of components in operation.
- **Recertification audits** on a three-year cycle, involving a proportionate re-assessment of both Stage 1 (policies and documentation) and Stage 2 (components and context of use).
- Accelerated monitoring or special audits where non-conformities, regulatory action or adverse findings are identified.

Superseded

2. Normative References

The following documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition (including amendments and corrigenda) applies.

These technical requirements are based on the framework established by:

- **ISO/IEC 27566-1:2025**, *Information security, cybersecurity and privacy protection — Age assurance systems — Part 1: Framework*

In addition, the following documents are normative references in these requirements:

- **IEEE 2089.1:2024**, *Online Age Verification Systems*
- **ISO/IEC 25000 series**, *Systems and software Quality Requirements and Evaluation (SQuaRE)* — for product quality characteristics.
- **ISO/IEC/IEEE 29119 series**, *Systems and software engineering — Software testing* — for selection of appropriate test methods.
- **ISO/IEC 30107 series**, *Biometric presentation attack detection* — where applicable to liveness detection and binding.
- **ISO/IEC 19795-1:2021**, *Biometric performance testing and reporting — Part 1: Principles and framework* — where applicable to the testing of biometric-based age estimation or verification.
- **ISO/IEC 42001:2023**, *Artificial intelligence management systems* — where applicable to AI-driven estimation.
- **ISO/IEC TR 24027:2021**, *Bias in AI systems and AI-aided decision-making* — where applicable to testing demographic fairness.
- **ISO/IEC 29115:2013**, *Entity authentication assurance framework* — where applicable to binding assurance results to individuals.
- **ISO/IEC 24760 series**, *Identity management framework* — where applicable to interoperability and secure exchange of results.
- **ACCS 0:2025**, *Age Check Certification Scheme — General Scheme Rules*.

Note: This list is not exhaustive. Other international standards may be identified and applied where relevant to the component or system under analysis. The certification process set out in this document requires auditors and evaluators to identify and apply the appropriate international standards when analysing a given component, considering its role, context of use and potential attack vectors (including but not limited to presentation, injection, synthetic media and iterative probing attacks).

Superseded

3. Terms and Definitions

In this document:

- **shall** indicates a requirement
- **should** indicates a recommendation
- **may** indicates a permission
- **can** indicates a possibility or a capability

Guidance notes are shown in italic text and are intended to assist the reader with understanding provisions. When referring to the ACCS Standards, refer to the ACCS Standard, followed by the year of issue, followed by the provision – such as ACCS 0:2024, 4.3.

The terms and definitions in **ISO/IEC 27566-1** and **IEEE 2089.1** shall apply.

In addition, the following terms and definitions are relevant to these technical requirements:

3.1 Certification Requirement

A specified requirement that is fulfilled by the client as a condition of establishing and maintaining certification.
[ISO/IEC 17065:2012 – 3.7]

3.2 Certification Scheme

The Age Check Certification Scheme (ACCS).
[ISO/IEC 17065:2012 – 3.9]

3.3 Client

An organisation that has applied for certification or been granted certification and is responsible to the conformity assessment body for ensuring that the certification requirements are fulfilled.
[ISO/IEC 17065:2012 – 3.1]

3.4 System or Component under Analysis

The defined system, subsystem or component presented for certification under this scheme, with explicit scope boundaries, contexts of use and version or deployment references.

3.5 Context(s) of Use

The declared operating environment(s) for a system or component under analysis, including sector(s), channel(s), use type (single-use or reusable) and jurisdiction(s).

3.6 Practice Statement

The formal claim made by a client, in accordance with ISO/IEC 27566-1 Clause 10 and Clause 5 of this scheme, describing the methods, outcomes,

Superseded

indicators of effectiveness, data dependencies and governance applied to the system or component under analysis.

3.7 Configuration Management

The documented process by which configuration settings of a system or component are identified, applied, controlled and maintained, in accordance with ISO 10007, including safeguards against relying party configurations that could compromise conformity.

3.8 Surveillance Audit

A periodic audit, conducted annually within ±30 days of the anniversary of certification, to confirm that the system or component under analysis continues to conform to certification requirements.

3.9 Recertification Audit

A comprehensive audit, conducted prior to expiry of a three-year certification cycle, to reassess conformity of the system or component under analysis against current scheme requirements.

3.10 Evaluation Review

The independent review of Stage One and Stage Two audit reports, practice statements and supporting evidence, carried out by personnel independent of the audit and testing team, to determine whether sufficient evidence exists to support the certification decision.

3.11 Certificate and Schedule of Certification

The formal certification documents issued by the conformity assessment body, comprising:
a) the certificate, confirming conformity with this scheme and identifying the client; and
b) the schedule of certification, detailing scope, contexts of use, indicators of effectiveness, data dependencies, assumptions, exclusions and limitations.

3.12 Continuous Monitoring

Ongoing review of the operational performance of a certified system or component, including automated monitoring where feasible, to detect changes in classification accuracy, demographic error parity, security, privacy or acceptability.

Superseded

4. Scope of the age assurance system under analysis or comparison

4.1 General

The scope of the age assurance system, service or component under analysis or comparison **shall be defined and recorded** in the certification agreement. The scope **shall identify the boundaries of the system or component** under analysis and the contexts of use in which certification is sought.

Certification may apply to:

- complete age assurance systems; or
- individual components (for example, verification, estimation, inference, binding, successive validation, liveness detection orchestration or delivery functions), provided they are defined as systems or components under analysis in accordance with this scheme.

Where certification applies to a component, the scope shall identify its role in the wider age assurance process and its interfaces with other systems or components.

4.2 Age Assurance Providers

Where the client is an age assurance provider, the scope shall include:

a) the name, including deployment or version reference, of the system or component under analysis;
b) the operating parameters, including:
    a. any process limitations;
    b. prerequisites for operation;
    c. tethering or connectivity requirements;
    d. technological dependencies;
    e. performance throttling or exclusions applied to outputs;
    f. whether the system operates online, offline or both;
    g. the goods, content, services, venues or spaces for which it is designed;
    h. the jurisdictions in which it is intended to operate (which may be global);
    i. whether age assurance results are intended for single-use or reusable contexts;
c) a technical architecture diagram showing the high-level interaction between the system or component under analysis and relevant parties (the individual, intermediaries, relying parties);
d) where applicable, identification of the international standards to be applied for testing and analysis of the component (e.g. ISO/IEC 29119 for test methodology, ISO/IEC 25000 for quality attributes, ISO/IEC 30107 for presentation attack detection).

4.3 Relying Parties

Where the client is a relying party, the scope shall include:

Superseded

a) the organisational footprint of the relying party, including where the system or component under analysis is deployed;
b) the goods, content, services, venues or spaces in which the system or component is deployed;
c) the age-related eligibility requirements established by the relying party (e.g. age limits or age bands);
d) the jurisdictions in which the relying party operates (which may be global);
e) any other relevant specifications, performance requirements, regulatory obligations or practical requirements specified by the relying party.

4.4 Intermediaries

Where the client is an intermediary, the scope shall include:

a) the name, including deployment or version reference, of the component or function under analysis;
b) the function performed by the intermediary, including its relationships and responsibilities toward providers, relying parties, individuals or other parties;
c) the process limitations, technological requirements or other parameters applicable to the component or function under analysis;
d) the jurisdictions in which the component or function operates (which may be global);
e) where applicable, identification of the relevant international standards and attack vectors to be addressed for the component under analysis.

4.5 Declaration of Threats and Attack Vectors

For all categories of client, the scope shall record any known or anticipated attack vectors relevant to the system or component under analysis, including but not limited to presentation attacks, injection attacks, deepfake/synthetic media attacks and iterative probing ("hill-climb") attacks.

4.6 Definition of Boundaries

The client **shall define the boundaries** of the system or component under analysis in a manner that enables repeatable certification. The boundary definition **shall include**:

a) a high-level architecture diagram identifying:
    a. the system or component under analysis;
    b. the interfaces with other systems, components or intermediaries;
    c. the flow of data and results between parties (individuals, intermediaries, relying parties);
    d. any dependencies on external systems or services.
b) documentary identification of:
    a. the name of the system or component;
    b. the version, issue or deployment reference;
    c. the date of release or deployment;
    d. the jurisdictions and contexts of use covered by this certification.
c) a statement of scope boundaries, which **shall specify**:
    a. what functions, processes or methods are included in the certification;
    b. what functions, processes or methods are explicitly excluded from certification;

Superseded

    c. any assumptions, prerequisites or conditions necessary for operation within the certified scope.
d) where relevant, reference to the applicable international standards or normative specifications against which each component within the boundary will be analysed.

The certification agreement **shall record** the defined boundaries of the system or component under analysis and the certificate and schedule of conformity **shall clearly state** the scope boundaries and version reference certified.

4.7 Contexts of Use

For every system or component under analysis, the client **shall define the contexts of use** for which certification is sought. The contexts of use **shall include, at a minimum**:

a) **Sector(s)** in which the system or component operates (for example: retail and convenience, licensed hospitality, gambling, regulated entertainment/social media and content, body modification or other).
b) **Channel(s)** of operation (offline, online or both).
c) **Intended use** of age assurance results (single-use or reusable).
d) **Jurisdiction(s)** of deployment, including:
    a. specific countries;
    b. regional groupings (such as EU, US, APAC); or
    c. global application.

The contexts of use **shall be documented** in the certification agreement and reflected in the certificate and schedule of conformity.

Where multiple contexts of use apply, the conformity assessment body **shall determine** whether testing, analysis and audit effort must be applied separately or in combination, considering sectoral requirements, jurisdictional regulations and risk of harm.

4.8 Ongoing Monitoring and Change Control

4.8.1 Certification Cycle

Certification shall be valid for a maximum period of **three years**.
During the certification cycle, the client shall undergo:

a) an **annual surveillance audit**, conducted within ±30 days of the anniversary of the initial certification decision; and
b) a **recertification audit** prior to expiry of the three-year cycle.

Surveillance and recertification audits shall include a review of:

a) current scope boundaries;
b) contexts of use;
c) changes to systems or components under analysis;
d) evidence of continued conformity with the scheme requirements.

Superseded

4.8.2 Automated Continuous Monitoring

Where technically feasible, the client shall support **automated continuous monitoring** of the use and effectiveness of the certified system or component. Automated monitoring may include:

a) telemetry or reporting on system performance and error rates;
b) monitoring of indicators of effectiveness across different demographics;
c) detection of anomalies or adverse events that may impact conformity;
d) logging of updates, upgrades or reconfiguration affecting the scope of certification.

4.8.3 Change Management

The client shall notify the conformity assessment body of any **material change** to a certified system or component, including:

a) **major version upgrades**;
b) **addition or removal of components**;
c) **changes to scope boundaries** (functions, processes or interfaces);
d) **changes to contexts of use** (sectors, channels, jurisdictions or use types).

Where a material change occurs, the conformity assessment body shall determine whether an **intervening audit** is required. Such an audit may be limited to the change in question.

Where a **minor change** occurs that does not materially affect the indicators of effectiveness, security, privacy or acceptability, the client may implement the change without prior audit. Such changes shall be documented and reviewed at the next surveillance audit.

4.8.4 Minor vs Major Change Parameters

A **minor change** is one that:

a) does not alter the classification accuracy level or indicators of effectiveness declared in the schedule of conformity;
b) does not introduce a new age assurance method or remove an existing one;
c) does not expand or reduce the defined scope boundaries or contexts of use;
d) does not materially alter privacy, security or acceptability characteristics.

A **major change** is any change that does not meet the definition of minor. Major changes require notification to the conformity assessment body within 30 days and may trigger an intervening audit.

4.8.5 Withdrawal or Suspension

Failure to notify the conformity assessment body of a major change or evidence that changes have compromised conformity, may result in the suspension, reduction or withdrawal of certification in accordance with the scheme rules.

4.9 Data Dependencies

The client **shall declare all data sources** utilised by the system or component under analysis. For each data source, the client **shall identify**:

a) whether it is an **authoritative source** (e.g. government-issued identity document, verified digital credential or accredited register);

Superseded

b) whether it is a **non-authoritative or secondary source** (e.g. credit reference, mobile network operator, social signals or self-asserted information);
c) any conditions, contractual arrangements or trust frameworks that govern the use of the data;
d) any dependencies on third-party services for access to or validation of the data.

The declaration of data dependencies **shall form part of the scoping documentation** and be reviewed at surveillance and recertification audits.

4.10 Assumptions and Exclusions

The client **shall declare any assumptions** that underpin the correct operation of the system or component under analysis. Such assumptions may include, but are not limited to:

a) environmental conditions (e.g. lighting levels, network connectivity, device capabilities);
b) demographic coverage (e.g. minimum dataset size or population representativeness);
c) operational practices (e.g. requirement for human oversight or fallback procedures).

The client **shall also declare any exclusions** from the scope of certification, such as:

a) explicit age groups for which the system or component is not intended (e.g. under 13s);
b) contexts of use not supported (e.g. offline use only, not suitable for mobile deployment);
c) functions or methods excluded from the certified boundary.

Declarations of assumptions and exclusions **shall be documented** in the certification agreement and referenced on the certificate and schedule of conformity, to ensure transparency and repeatability of certification.

Superseded

5. Practice Statements

5.1 General Requirements

All clients seeking certification **shall produce a practice statement** in accordance with ISO/IEC 27566-1, Clause 10.

The practice statement **shall represent the client's formal claim** of conformity and serve as the primary basis for assessment under this scheme.

The practice statement **shall be made publicly available** unless restricted by law or regulatory requirement, in which case an executive summary shall be published.

5.2 Content of Practice Statements

5.2.1 Core Content Requirements

The practice statement **shall, at a minimum**, contain the elements required by ISO/IEC 27566-1, Clause 10. These include:

a) description of the required age-related eligibility outcomes;
b) description of methods used (verification, estimation, inference, binding, successive validation);
c) description of sources of data (authoritative and non-authoritative);
d) indicators of effectiveness achieved;
e) privacy and data protection measures;
f) security protections against relevant attack vectors (in outline, not detail);
g) usability, inclusivity and acceptability considerations;
h) governance, oversight and audit arrangements.

Where applicable, the practice statement **shall identify** the relevant international standards applied for testing or analysis of the system or component under analysis.

5.2.2 Additional Content Requirements

In addition to the elements specified in ISO/IEC 27566-1, Clause 10, the practice statement **shall declare**:

a) the identified needs of relying parties that the system or component is intended to meet;
b) the sources of data used, distinguishing authoritative sources from non-authoritative or secondary sources and the management of those dependencies;
c) how the system or component ensures the correct handling of date information;
d) the functional characteristics of the system or component, including suitability, completeness, correctness and appropriateness;
e) the claimed classification accuracy level (Basic, Effective, Highly Effective, Strict) for each component or for the system as a whole;
f) any publicly available specifications with which the client asserts conformity;
g) performance efficiency claims, including intended time, throughput, resource utilisation and capacity parameters.

Superseded

5.3 Basis for Assessment

The practice statement **shall be assessed** by the conformity assessment body against the five core characteristics defined in ISO/IEC 27566-1 (functionality, performance, privacy, security, acceptability).

The assessment **shall determine** whether the claims made in the practice statement are:

a) supported by evidence from testing, analysis and audit;
b) consistent with the scope boundaries and contexts of use declared under Clause 4;
c) aligned with the normative references and scheme requirements.

5.4 Updates and Maintenance

The client **shall review and update** the practice statement at least annually.

The client **shall update** the practice statement whenever:

a) a major change occurs under Clause 4.8 (Ongoing Monitoring and Change Control); or
b) a change materially affects functionality, performance, privacy, security or acceptability characteristics.

Updated practice statements **shall be submitted** to the conformity assessment body for review.

5.5 Structured Submission

Clients may use the **ACCS Practice Statement Tool**, available on the scheme website, to assist in structuring their practice statement.

Use of the tool is **optional**, but any practice statement submitted **shall follow** the standardised structure set out in ISO/IEC 27566-1, Clause 10, to ensure comparability and repeatability of certification.

5.6 Auditor Responsibilities

Auditors **shall review** the practice statement for completeness and consistency as part of Stage 1 (policy audit).

Auditors **shall verify** that evidence provided during Stage 2 (component and context audit) substantiates the claims made in the practice statement.

Any gaps, inconsistencies or unsupported claims **shall be raised** as nonconformities.

5.7 Configuration Management

The practice statement **shall declare** the approach taken to configuration management in accordance with ISO 10007, including:

a) how configuration items are identified and controlled;
b) how changes are evaluated, authorised and implemented;
c) how configuration status is recorded and reported;
d) how configuration audits are conducted.

The practice statement **shall identify** whether configuration settings are:

Superseded

a) applied solely by the age assurance provider; or
b) capable of being applied or altered by relying parties (for example, via a client dashboard).

Where relying parties are permitted to apply or alter configuration settings, the practice statement **shall describe**:

a) the safeguards in place to prevent configurations that would compromise conformity with ISO/IEC 27566-1 requirements;
b) how security, privacy and acceptability characteristics are preserved under permitted configurations;
c) what controls exist to prevent reduction of efficacy (for example, lowering thresholds, disabling liveness checks or bypassing privacy-preserving features).

The conformity assessment body **shall assess** whether the declared configuration management approach is sufficient to maintain conformity throughout the certification cycle, including during version upgrades or when relying parties exercise configuration options.

Any configuration options that could reduce the indicators of effectiveness or remove essential privacy or security controls, **shall be explicitly prohibited** or technically constrained by the provider.

5.8 Change Control, Documentation and Record Keeping

The practice statement **shall identify the authority** within the client organisation responsible for approving, updating and maintaining the practice statement.

Changes to the practice statement **shall be documented**, including:

a) the nature of the change;
b) the rationale for the change;
c) the date of approval;
d) the approving authority.

The client **shall maintain records** of all versions of the practice statement issued during the certification cycle. Records shall be retained for a minimum of six years or two certification cycles, whichever is longer.

The practice statement **shall include a version reference and date of issue**. The current version shall always be clearly identifiable as the operative version.

Where changes to the practice statement reflect a **major change** to the system or component under analysis (as defined in Clause 4.8), the updated practice statement **shall be submitted** to the conformity assessment body within 14 days of the approved change.

Minor or editorial changes that do not materially affect conformity or indicators of effectiveness may be documented internally and reviewed at the next surveillance audit.

5.9 Recognition of Other Certifications and External Evidence

The practice statement **may declare** conformity with other certifications, accreditations or component test results relevant to the system or component under analysis. Such evidence may include, but is not limited to:

Superseded

a) certification to international management system standards (e.g. ISO 9001, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 42001);
b) product or component certifications issued under ISO/IEC 17065 schemes (e.g. ISO/IEC 30107 for biometric presentation attack detection);
c) independent conformity assessments issued by accredited conformity assessment bodies;
d) other external audit or test reports.

The auditor **shall assess the relevance, credibility and applicability** of such evidence to the requirements of this scheme and to ISO/IEC 27566-1.

The following weighting policy applies to external evidence:

1. **Evidence from an ILAC/IAF/EA Member Body Accredited CAB, within scope of accreditation**
   – Substantial weight is given. The auditor shall confirm the validity of the certificate, the standards applied and the mapping to scheme requirements.

2. **Evidence from an ILAC/IAF/EA Member Body Accredited CAB, outside scope of accreditation**
   – Significant weight is given. The auditor shall verify the CAB's impartiality and competence but may require clarification of the standards or methods applied.

3. **Evidence from a non-ILAC/IAF/EA Member Body Accredited CAB**
   – Limited weight is given. The auditor shall review the full audit or test reports and determine if the evidence is sufficient or if further testing is required under this scheme.

4. **Evidence from other second-party or external sources** (e.g. consultant reports, SOC 2, independent reviews)
   – Treated as internal audit evidence. May be considered, but only limited weight is given.

Recognition of external certifications or test results **does not constitute automatic conformity** under this scheme. All evidence shall be reviewed objectively and conformity shall only be established where evidence is mapped to the requirements of ISO/IEC 27566-1 and these scheme rules.

Superseded

5.10 External Certification Change Notification

Where a client's practice statement declares conformity with another certification, accreditation or test result (as set out in Clause 5.9), the client **shall notify the conformity assessment body within 14 days** if that external certification or accreditation is:

a) suspended, reduced in scope, withdrawn or expired;
b) subject to regulatory action or adverse findings that affect its validity; or
c) materially changed such that the scope of the external certification no longer covers the declared functions, processes or components.

Such changes **shall be treated as a major change** under Clause 4.8 (Ongoing Monitoring and Change Control). The conformity assessment body **shall determine** whether an intervening audit is required to confirm continued conformity of the system or component under analysis.

6. Stage One Audit

6.1 Purpose

The Stage One audit is intended to:

a) confirm that the client has produced a practice statement in accordance with Clause 5;
b) assess the adequacy of the practice statement and supporting documentation against the five core characteristics (functionality, performance, privacy, security, acceptability);
c) determine whether the client is ready to proceed to Stage Two (system and component analysis).

6.2 Scope of Review

The Stage One audit **shall include, at a minimum**:

a) verification that the practice statement is complete, current, approved and publicly available (or that a public summary has been provided);
b) review of governance, authority and record-keeping processes relating to the practice statement (Clause 5.8);
c) confirmation of declared scope boundaries, contexts of use and data dependencies (Clause 4.6–4.9);
d) confirmation of declared assumptions and exclusions (Clause 4.10);
e) review of configuration management approach, including whether configuration settings are controlled solely by the provider or may be altered by relying parties (Clause 5.7);
f) review of change control processes, including how minor and major changes are documented and notified (Clause 4.8 and Clause 5.10);
g) review of external evidence cited (Clause 5.9) and determination of its credibility, relevance and applicability.

Superseded

6.3 Legal and Regulatory Requirements

The Stage One audit **shall confirm** that:

a) the client is a legally constituted entity in its jurisdiction(s) of operation;
b) the client is free from restrictions that would prohibit operation of the system or component under analysis;
c) any regulatory approvals, licences or authorisations required for operation in relevant jurisdictions are identified and current;
d) any enforcement actions, sanctions or investigations by supervisory or regulatory authorities in relevant jurisdictions are disclosed.

6.4 Impartiality and Conflicts of Interest

The Stage One audit **shall confirm** that:

a) the conformity assessment body has no consultancy relationship with the client, in line with ISO/IEC 17065 impartiality requirements;
b) the client has disclosed any known conflicts of interest that could undermine certification integrity.

6.5 Privacy and Data Protection Baseline

The Stage One audit **shall confirm** that:

a) the practice statement addresses data protection and privacy obligations applicable in the jurisdictions of use;
b) the system or component under analysis demonstrates adherence to recognised privacy frameworks (for example, ISO/IEC 27701, ISO/IEC 29100, GDPR or equivalent national laws);
c) mechanisms exist for handling data subject rights, including access, correction, erasure and redress where required by applicable law.

6.6 Risk Management and Attack Vectors

The Stage One audit **shall confirm** that:

a) the client has considered risks relevant to the system or component under analysis, including misuse scenarios and harms to individuals;
b) declared assumptions and exclusions (Clause 4.10) are risk-based and justified;
c) the practice statement identifies relevant attack vectors (Clause 4.5) and how these are mitigated.

6.7 Management System Readiness

The Stage One audit **shall confirm** whether the client operates recognised management systems (e.g. ISO 9001, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 42001) and whether these are accredited under ILAC/IAF/EA or equivalent bodies.

Where such certifications exist, the audit **shall determine** their relevance and weight in accordance with Clause 5.9.

6.8 Monitoring and Continuous Improvement

The Stage One audit **shall confirm** that the client has processes in place for:

a) ongoing monitoring of the use and effectiveness of the system or component under analysis, including automated monitoring where feasible;
b) internal review and continual improvement of conformity with the scheme;
c) timely notification of major changes (Clause 4.8).

6.9 Outcomes of Stage One Audit

If Stage One audit confirms readiness, the client **shall proceed to Stage Two**.

Where gaps, inconsistencies or unsupported claims are identified, the conformity assessment body **shall issue nonconformities** to be addressed before Stage Two can commence.

The Stage One audit report **shall record** the findings, nonconformities and determination of readiness.

Superseded

7. Selection and Specification of Testing

7.1 Purpose

The purpose of this clause is to ensure that testing and analysis of age assurance systems and components is undertaken in a systematic, repeatable and internationally recognised manner, aligned with ISO/IEC/IEEE 29119, ISO/IEC 25000, ISO/IEC 19795, ISO/IEC 30107, IEEE 2089.1 and ISO/IEC 27566-3 (draft).

7.2 Competence of Test Analysts

Test analysts **shall be demonstrably competent** in:

a) software and systems testing in accordance with ISO/IEC/IEEE 29119;
b) application of the ISO/IEC 25000 product quality model;
c) biometric testing where applicable (ISO/IEC 19795, ISO/IEC 30107);
d) statistical methods for determining sample sizes, classification accuracy and error rates.

Test analysts **shall be independent** of the system or component under analysis. Test analysts can be internal to the conformity assessment body or outsourced in accordance with ISO/IEC 17065.

7.3 Development of Test Plans

The client's practice statement (Clause 5) **shall form the basis** of the test plan.

The conformity assessment body **shall ensure** that each test plan:

a) specifies the scope and objectives of testing;
b) identifies the components, functions or characteristics to be tested;
c) maps each declared claim in the practice statement to a corresponding test or analysis;
d) specifies acceptance criteria for each test, linked to indicators of effectiveness.

Test plans **shall be reviewed and approved** by the conformity assessment body during Stage One audit (Clause 6).

Superseded

7.4 Test Selection

Functional and performance testing **shall be designed** using ISO/IEC/IEEE 29119 test design techniques, selected in accordance with the nature of the system or component under analysis.

Test coverage **shall include, at a minimum**:

a) functional suitability, completeness, correctness and appropriateness;
b) classification accuracy;
c) performance efficiency (response time, throughput, scalability);
d) resistance to relevant attack vectors (presentation, injection, deepfake, replay, hill-climb);
e) privacy, security and acceptability characteristics as declared in the practice statement.

7.5 Sample Size and Demographics

Subject to Clause 7.11 to 7.14, sample sizes **shall be proportionate** to the claimed indicator of effectiveness (Basic, Effective, Highly Effective, Strict).

Minimum expectations:

a) Basic: ≥ 30 test subjects, classification accuracy ≥ 80%;
b) Effective: ≥ 300 test subjects in one demographic group, classification accuracy ≥ 90%;
c) Highly Effective: ≥ 300 subjects in each of at least three skin tones and both genders, classification accuracy ≥ 95%;
d) Strict: ≥ 3,000 test subjects across multiple demographics and environments, classification accuracy ≥ 99%.

Test populations **shall include** variation in age, gender, skin tone, accessibility needs and environmental conditions, unless exclusions are justified and declared under Clause 4.10.

7.6 Indicators of Effectiveness

Indicators of effectiveness **shall be determined** for each component and for the system as a whole, as applicable.

Test results **shall demonstrate** conformity with the indicator of effectiveness claimed in the practice statement.

Where a component achieves differing indicators of effectiveness, the certification schedule **shall specify** the level achieved for each component.

7.7 National and Jurisdictional Requirements

Where national regulators specify minimum test requirements (e.g. demographic fairness, attack vector resilience or sector-specific conditions), those requirements **shall be applied** in addition to this clause.

The conformity assessment body **shall record** in the certification agreement which national or regional requirements have been applied.

The certification scheme **shall maintain** a record of approved national or jurisdictional requirements in supplementary documents as applicable.

7.8 Documentation and Records

Each test plan **shall include**:

a) objectives and scope;
b) test methods selected and justification;
c) sample sizes and demographics;
d) acceptance criteria;
e) handling of attack vectors;
f) any national requirements applied.

Test results **shall be documented** in a test report, retained by the conformity assessment body and subject to independent evaluation review (Clause 9).

Superseded

The certificate and schedule of conformity **shall state** the classification accuracy and indicator of effectiveness achieved and any limitations of testing.

7.9 Recognition of External Testing

Clients may submit results from external testing of systems or components under analysis. Such testing **shall be conducted** in accordance with internationally recognised standards (e.g. ISO/IEC 19795, ISO/IEC 30107, ISO/IEC/IEEE 29119, IEEE 2089.1) and aligned with the requirements of this clause.

The conformity assessment body **shall assess** the credibility, independence and relevance of such test results in accordance with the recognition policy set out in Clause 5.9.

Where external testing has been conducted by a conformity assessment body accredited by an ILAC/IAF/EA member in scope of that accreditation, **substantial weight** shall be given.

Where testing has been conducted outside of accreditation or by non-accredited laboratories, the conformity assessment body **shall determine** whether additional confirmatory testing or review is required.

7.10 Outsourced Testing to Approved Laboratories

The conformity assessment body may outsource testing activities to **approved test laboratories** where this is necessary to complete Stage Two analysis.

Approved test laboratories **shall demonstrate competence** in the application of relevant ISO/IEC/IEEE standards and methods and operate to recognised management system principles (e.g. ISO/IEC 17025 or ISO/IEC 17065 as applicable).

The conformity assessment body **shall retain full responsibility** for the certification decision and all outsourced testing shall be conducted under the authority of this scheme.

Approved laboratories **shall be subject to monitoring** by the conformity assessment body to ensure continued competence, impartiality and alignment with this scheme.

7.11 Statistical Assurance Framework (Alternative Evidence Models)

Test plans may use **sequential or adaptive designs** (e.g., group-sequential, SPRT) to minimise sample sizes while maintaining pre-specified type I/II error rates.

Performance claims **shall be framed as non-inferiority/equivalence** against the indicator threshold (e.g., ≥95%), evaluated via one-sided confidence intervals (frequentist) or posterior credible intervals (Bayesian) with pre-declared priors.

Demographic reporting **shall use stratified analyses**. Hierarchical (multilevel) models may be used to **borrow strength** across strata, but **stratum-specific lower bounds** (CI/CrI) **shall still be reported** and compared to local/jurisdictional minima where applicable.

The test plan **shall pre-register**: endpoints, thresholds, margins (Δ), stopping rules, analysis method (CI/CrI type), priors (if Bayesian), alpha/coverage, stratification and handling of missing data.

Superseded

Risk-based sampling shall set minimum per-stratum floors (see 7.12) and allocate additional samples to higher-risk strata (e.g., younger cohorts, accessibility groups, under-represented skin tones).

Where **external evidence** (Clauses 5.9, 7.9) or **operational monitoring data** (Clause 4.8.2) is used to reduce new sampling, the test plan shall show data lineage, quality controls and statistical integration (e.g., meta-analytic priors, propensity controls).

7.12 Minimum Stratified Floors (when using reduced-N designs)

As a default (may be superseded by national rules):

- **Basic**: total ≥60; per key stratum ≥10
- **Effective**: total ≥150; per key stratum ≥25
- **Highly Effective**: total ≥400; per key stratum ≥50 across ≥3 skin tone groups and ≥2 genders
- **Strict**: total ≥1,000; per key stratum ≥100 across ≥3 skin tones, ≥2 genders and ≥2 device types

Key strata shall reflect declared contexts of use and known risk factors (age bands, gender, skin tone, accessibility, device/channel).

7.13 Acceptance Rules (examples)

Non-inferiority: Accept "Effective (95%)" if the **one-sided 95% lower CI** for accuracy ≥ 95.0%.

Sequential early stop (success): Stop early if interim lower bound ≥ threshold + δ (pre-set); otherwise continue to next look.

Fairness: Report **per-stratum lower bounds**; flag if any falls below local minimum. Require mitigation plan or scope limitation.

Operational corroboration: Where automated monitoring shows sustained performance ≥ threshold with control-limits (e.g., CUSUM), allow **reduced confirmatory sample** at recertification.

7.14 Data Integrity & Anti-gaming Controls

Use **data locking/splitting** (design vs confirmatory sets) for vendor-supplied datasets.

Prohibit "peeking" outside pre-declared interim looks.

Record full **traceability** (datasets, seeds, code version, environment) so results are reproducible.

Superseded

8. Execution of Testing and Reporting of Analysis

8.1 Purpose

The purpose of this clause is to ensure that testing of systems and components under analysis is conducted in accordance with approved test plans (Clause 7) and that the results are reported in a complete, consistent and comparable manner to the conformity assessment body.

8.2 Execution of Testing

Testing **shall be conducted** in accordance with the approved test plan reviewed at Stage One (Clause 6).

Test analysts **shall document** all deviations from the plan, including justifications and impacts on results.

Testing **shall be repeatable and reproducible**, with sufficient records to allow an independent reviewer to verify the validity of results.

Test data and environments **shall be controlled**, documented and retained for audit.

8.3 Analysis of Results

Test results **shall be analysed** against the declared indicators of effectiveness (Basic, Effective, Highly Effective, Strict) for each component and the system as a whole.

Analysis **shall include**:

a) classification accuracy and error rates (false positives/negatives, outcome error parity);
b) performance efficiency (response time, throughput, resource use);
c) resilience against relevant attack vectors (Clause 4.5);
d) privacy, security and acceptability characteristics.

Where external or outsourced testing is used (Clauses 7.9–7.10), the analysis **shall clearly identify** the source of results and the weight given.

Superseded

8.4 Reporting of Results

Test reports **shall be prepared** in accordance with international reporting standards, including:

a) ISO/IEC/IEEE 29119-3 (*Software and systems testing — Test documentation*);
b) ISO/IEC 25062 (*Common Industry Format for usability test reports*), where applicable;
c) ISO/IEC 19795-4 (*Biometric performance testing and reporting*), where applicable;
d) ISO/IEC 30107-3 (*Presentation attack detection — Testing and reporting*), where applicable.

Test reports **shall include, at a minimum**:

a) objectives and scope of testing;
b) test environment, data sets and configurations used;
c) methods applied and justification for their selection;
d) sample sizes and demographics;

e) raw and analysed results, including statistical confidence intervals;
f) nonconformities or deviations observed, including any inconsistencies with practice statements;
g) conclusion against indicators of effectiveness and acceptance criteria.

8.5 Reporting at Component Level

Test results **shall be reported separately for each component** under analysis, as well as for the system as a whole where applicable.

Component-level reporting **shall specify**:

a) the function tested (e.g. verification, estimation, inference, binding, delivery);
b) the indicator of effectiveness achieved;
c) any limitations of scope or context.

The certification schedule **shall reflect** these component-level results.

8.6 Submission to Conformity assessment body

Test reports **shall be submitted** to the conformity assessment body in full, together with any supporting evidence.

The conformity assessment body **shall review** the reports for completeness, accuracy and alignment with the practice statement.

Summaries of test results **shall be published** or made publicly available, unless restricted by legitimate confidentiality or legal grounds.

Superseded

9. Stage Two Audit (Specific Requirements)

9.1 Purpose

The Stage Two audit is intended to confirm, by direct audit and review of evidence, that the system or component under analysis conforms to the requirements of this scheme, ISO/IEC 27566-1 and relevant normative standards.

9.2 Mandatory Audit Activities

The Stage Two audit **shall include, at a minimum**:

a) **Verification of Test Results**
    a. Cross-check of reported results (Clause 8) against raw data, logs and configuration records.
    b. Spot-check replication of tests where feasible.
b) **Observation of Operation**
    a. Demonstration of system or component operation in a representative environment.
    b. Validation that system outputs correspond with practice statement claims.
c) **Sampling of Records**
    a. Review of user logs, audit trails, monitoring records and error handling.
    b. Confirmation of retention, integrity and accessibility of audit data.

d) **Interviews and Walkthroughs**
    a. Interviews with key staff (technical leads, privacy officers, system administrators).
    b. Walkthroughs of configuration settings, data flows and fallback mechanisms.
e) **Review of Interfaces**
    a. Examination of interfaces between the system or component and intermediaries, relying parties or external data sources.
    b. Confirmation of controls on data exchange and integrity.

9.3 Evidence Requirements

Clients **shall make available** for Stage Two audit:

a) full test reports and raw test data (Clause 8.4);
b) system or component configuration records and change logs;
c) operational logs demonstrating real-world performance;
d) monitoring outputs (including automated continuous monitoring where implemented);
e) records of privacy and security incidents, breaches or complaints in the certification cycle;
f) documentation of fallback and error-handling mechanisms;
g) training and competence records of relevant personnel.

9.4 Conformity Assessment Criteria

Auditors **shall determine** conformity with:

a) **Functionality**
    a. Evidence that the system performs the declared functions consistently under specified conditions.
    b. Confirmation that functional requirements in the practice statement are met.
b) **Performance**
    a. Evidence that classification accuracy thresholds are achieved (Basic, Effective, Highly Effective, Strict).
    b. Evidence of response time, throughput and scalability performance as claimed.
c) **Privacy**
    a. Evidence of data minimisation, lawful basis for processing, retention periods, rights management.
    b. Confirmation of alignment with ISO/IEC 27701 or equivalent frameworks, where claimed.
d) **Security**
    a. Evidence of controls against attack vectors (presentation, injection, deepfake, hill-climb, replay).
    b. Penetration test or red-team evidence where applicable.
e) **Acceptability**
    a. Evidence of accessibility, inclusivity and usability testing (e.g. CIF usability report).
    b. Evidence of complaints and redress mechanisms.

Superseded

9.5 Component and System-Level Requirements

Each component under analysis **shall be audited** separately, with indicators of effectiveness recorded.

System-level audit **shall confirm** that integration of components delivers outcomes consistent with relying party requirements.

9.6 Jurisdictional and Sectoral Requirements

Where deployment covers multiple jurisdictions, the Stage Two audit **shall confirm** compliance with local laws, regulations or standards declared in the scope.

Sector-specific obligations (e.g. gambling, social media, retail) **shall be assessed** for conformity.

9.7 Audit Findings and Reporting

All findings **shall be documented** in the Stage Two audit report, including:

a) conformities;
b) nonconformities (major and minor);
c) observations and recommendations;
d) limitations and exclusions.

Nonconformities **shall be categorised** (major/minor) and corrective actions required before certification decision.

The Stage Two audit report **shall explicitly map** each claim in the practice statement (Clause 5) to supporting evidence reviewed in Stage Two.

Superseded

10. Reporting of Indicators of Effectiveness

10.1 Purpose

This clause establishes requirements for reporting the indicators of effectiveness achieved by systems and components under analysis. Indicators of effectiveness provide a transparent measure of functional and performance outcomes, enabling comparability across systems, components and jurisdictions.

10.2 General Requirements

Indicators of effectiveness **shall be determined** on the basis of approved test plans (Clause 7), test execution and reporting (Clause 8) and Stage Two audit findings (Clause 9).

Indicators of effectiveness **shall be reported** for each certified component and, where applicable, for the integrated system as a whole.

Indicators of effectiveness **shall be recorded** on the certificate and schedule of conformity, together with scope boundaries, version references and declared contexts of use.

Summaries of indicators of effectiveness **shall be made publicly available**, subject to legitimate confidentiality or legal restrictions.

10.3 Levels of Effectiveness

Indicators of effectiveness **shall be expressed** at one of the following levels:

- **Basic** — classification accuracy ≥ 80%; testing with ≥ 30 subjects; suitable only for low-risk applications.
- **Effective** — classification accuracy ≥ 90%; testing with ≥ 300 subjects in one demographic group; suitable for moderate-risk applications.
- **Highly Effective** — classification accuracy ≥ 95%; testing with ≥ 300 subjects in at least three skin tone groups and both genders; suitable for high-risk applications.
- **Strict** — classification accuracy ≥ 99%; testing with ≥ 3,000 subjects across multiple demographics and environments; suitable for very high-risk applications.

These levels **shall be applied** to both individual components and to system-level results, unless excluded under Clause 4.10.

10.4 Statistical Basis

Indicators of effectiveness **shall be established** using statistically valid methods. Acceptable methods include:

a) fixed-sample designs meeting the minimum expectations in 10.3;
b) sequential or adaptive designs (e.g. group-sequential, SPRT), provided type I/II error rates are pre-specified and controlled;
c) non-inferiority or equivalence tests against the threshold (e.g. ≥95%) using one-sided confidence or credible intervals;
d) hierarchical or Bayesian models, provided that **stratum-specific lower bounds** are reported and compared against thresholds.

Acceptance rules **shall be pre-registered** in the test plan (Clause 7.13) and disclose: confidence/credibility level, thresholds, stopping rules, priors (if Bayesian) and handling of missing data.

Reduced sample sizes may be used where sequential/adaptive designs or operational monitoring evidence demonstrate conformity with controlled error rates.

Superseded

10.5 Component and System-Level Reporting

Indicators of effectiveness **shall be reported separately** for each component under analysis (e.g. verification, estimation, inference, binding, delivery).

System-level indicators of effectiveness **shall be reported** as the aggregate outcome, considering integration, configuration and contexts of use.

Where components achieve different indicators of effectiveness, these **shall be specified** in the certification schedule.

10.6 Demographic and Contextual Reporting

Indicators of effectiveness **shall disclose** demographic coverage, including gender, skin tone, age bands, accessibility needs and environmental conditions, where relevant.

Outcome error parity **shall be assessed** and where disparities exist between demographic groups, these **shall be declared** in the audit report and schedule of conformity.

Indicators of effectiveness **shall specify** whether results apply globally or are limited to specific jurisdictions or contexts of use (Clause 4.7).

10.7 Local Indicators of Effectiveness

Where local regulators or national standards bodies specify additional indicators of effectiveness, these **shall be reported** alongside the global indicators.

Such local indicators may include:

a) minimum thresholds for demographic fairness;
b) sector-specific thresholds (e.g. gambling, online content, retail);
c) fallback or successive validation requirements.

Local indicators **shall be clearly identified** as jurisdiction-specific and recorded on the certificate and schedule of conformity.

10.8 Reporting Format

Indicators of effectiveness **shall be presented** in a standardised reporting table, including:

a) component/system name and version;
b) indicator of effectiveness achieved (Basic/Effective/Highly Effective/Strict);
c) classification accuracy and error rates with confidence/credible bounds;
d) sample size and demographic coverage;
e) applicable contexts of use and jurisdictions;
f) local indicators (if applicable);
g) limitations, assumptions and exclusions.

11. Audit Report on Stage Two and Preparation for Evaluation Review

11.1 Purpose

The purpose of the audit report is to provide a comprehensive record of the Stage Two audit, documenting all findings, evidence and nonconformities and to prepare the evidence base for the evaluation review and certification decision.

11.2 General Requirements

The audit report **shall be produced** by the lead auditor following completion of the Stage Two audit.

The audit report **shall be prepared** in accordance with ISO/IEC 17065, ISO/IEC 17021-1 (as applicable to audit reporting) and ISO/IEC/IEEE 29119-3 (test documentation standards).

The audit report **shall be reviewed** internally by the conformity assessment body for completeness and accuracy before being submitted for evaluation review.

Superseded

11.3 Content of the Audit Report

The audit report **shall include, at a minimum**:

a) **Administrative Details**
   a. client name and legal entity details;
   b. scope of certification (system or component under analysis, version, deployment reference, date of release);
   c. contexts of use (sector, channel, single use/reusable, jurisdictions);
   d. certification agreement reference.

b) **Practice Statement Cross-Reference**
   a. confirmation of receipt and review of the practice statement (Clause 5);
   b. mapping of each claim in the practice statement to supporting evidence reviewed in Stage Two.

c) **Test Results**
   a. summary of test plans approved (Clause 7) and executed (Clause 8);
   b. summary of test results, including indicators of effectiveness achieved;
   c. supporting references to full test reports.

d) **Audit Findings by Core Characteristic**
   a. functionality;
   b. performance;
   c. privacy;
   d. security;
   e. acceptability.

   Each section **shall document** conformity, nonconformities (major/minor), observations and limitations.

e) **Component and System-Level Findings**
   a. indicators of effectiveness for each component;
   b. system-level indicators of effectiveness;
   c. integration and interoperability findings.

f) **National and Local Requirements**
   a. confirmation of compliance with jurisdictional or sectoral requirements;
   b. any local indicators of effectiveness reported (Clause 10.7).

g) **Nonconformities and Corrective Actions**
   a. list of nonconformities identified, categorised as major or minor;
   b. corrective action plans agreed with client;
   c. timelines for resolution.

h) **Supporting Evidence**
   a. references to records examined (logs, monitoring data, complaints handling, config management records, etc.);
   b. references to external certifications or testing relied upon (Clause 5.9).

i) **Auditor Declarations**
   a. confirmation of impartiality and independence;
   b. competence declarations of the audit team;
   c. date(s) of audit and personnel involved.

Superseded

11.4 Preparation for Evaluation Review

The audit report **shall be compiled** together with supporting documents (practice statement, test reports, nonconformity records) as the audit package for evaluation review (Clause 12).

The audit package **shall be checked** by the conformity assessment body to confirm completeness, consistency and traceability of evidence.

Any outstanding nonconformities **shall be addressed** and verified closed before submission to evaluation review, unless the conformity assessment body applies conditional acceptance in line with scheme rules.

The audit package **shall be version-controlled** and securely stored for a minimum of six years or two certification cycles, whichever is longer.

11.5 Reporting Format

The conformity assessment body **shall use a standardised audit report template**, included as Annex E (informative), to ensure consistency across all Stage Two audits.

The audit report template **shall include** sections for each of the required content areas in Clause 11.3.

The conformity assessment body **shall ensure** that the audit report is sufficiently detailed to support an independent evaluation review without the need for clarification from the audit team.

Superseded

12. Evaluation Review and Certification Decision

12.1 Purpose

The evaluation review and certification decision are intended to ensure that certification is granted only where sufficient objective evidence demonstrates conformity with the requirements of this scheme, ISO/IEC 27566-1 and other applicable standards.

12.2 Evaluation Review

The evaluation review **shall be conducted** by competent personnel independent of the audit and testing team.

The evaluation review **shall consider**:

a) the practice statement and updates (Clause 5);
b) the approved test plan (Clause 7) and test reports (Clause 8);
c) the Stage Two audit report and supporting evidence (Clause 11);
d) indicators of effectiveness achieved (Clause 10);
e) any nonconformities and corrective actions.

The evaluation review **shall confirm**:

a) that the scope boundaries and contexts of use are correctly defined and documented;
b) that all five core characteristics (functionality, performance, privacy, security, acceptability) have been assessed;

c) that indicators of effectiveness are reported at both component and system level;
d) that local or jurisdictional requirements are addressed where applicable;
e) that all nonconformities have been resolved or subject to an agreed corrective action plan.

The outcome of the evaluation review **shall be documented** and form the basis of the certification decision.

12.3 Certification Decision

The certification decision **shall be made** by the certification officer(s) authorised by the conformity assessment body, independent from the auditors and test analysts.

The certification decision **shall determine** whether to:

a) grant certification;
b) grant certification subject to conditions;
c) defer certification pending corrective actions;
d) refuse certification.

Certification decisions **shall be documented** and recorded in the conformity assessment body's management system.

Clients **shall be informed** in writing of the certification decision, including reasons where certification is refused or deferred.

12.4 Certificate and Schedule of Certification

Where certification is granted, the conformity assessment body **shall issue** a certificate and accompanying schedule of certification.

The certificate and schedule of certification **shall clearly distinguish** between:

a) what is certified (defined scope, components, indicators, contexts of use); and
b) what is not certified (functions excluded, untested contexts, unsupported claims).

12.4.1 Certificate of Conformity

The certificate **shall include**:

a) the product, component or system under analysis;
b) the name and legal identity of the client;
c) reference to this scheme (ACCS 1:2025) and ISO/IEC 27566-1;
d) a unique certificate number;
e) date of issue and expiry;
f) authorised signatory;

12.4.2 Schedule of Certification

The schedule of certification **shall include**:

a) the name, version and deployment reference of the system or component under analysis;
b) scope boundaries and contexts of use (Clause 4.6–4.7);

Superseded

c) indicators of effectiveness achieved for each component and at system level (Clause 10);
d) assumptions and exclusions (Clause 4.10);
e) data dependencies (Clause 4.9);
f) any local or jurisdictional indicators applied;
g) limitations of certification (e.g. where components are excluded from scope or where results apply only in specified contexts).

12.5 Public Registry and Use of Marks

Certified clients **shall be entered** into the public registry maintained by the conformity assessment body.

The scope and schedule of certification **shall be publicly accessible**, except where legal or confidentiality restrictions apply.

Use of the certification mark **shall be limited** to the certified scope and subject to the scheme's rules of use (as set out in ACCS 0:2025).

Certified clients of any conformity assessment body may be additionally listed in the ACCS registry.

12.6 Optional Subsequent Certification by IEEE

Clients who have successfully obtained certification under this scheme may, if they choose, seek subsequent certification under the IEEE 2089.1 certification scheme.

Where the client opts for subsequent IEEE certification, the conformity assessment body **shall provide**:

a) the audit package (practice statement, test reports, audit report, evaluation review) in the format required by IEEE;
b) confirmation of the scope, contexts of use and indicators of effectiveness achieved under this scheme;
c) any limitations, assumptions or exclusions recorded in the schedule of conformity.

The client **shall be responsible** for submitting the required documentation to IEEE and for meeting any additional requirements set out in the IEEE scheme.

Certification under this scheme and certification under the IEEE scheme are **separate and independent**. Certification to this scheme does not automatically constitute certification to IEEE 2089.1 and vice versa.

Where the client obtains certification under IEEE 2089.1, the conformity assessment body may, with the client's consent, cross-reference the IEEE certification in the ACCS registry.

Clients obtaining IEEE certification may also be listed in the **IEEE registry**, subject to IEEE's rules and procedures.

Superseded

13. Continuous Monitoring and Surveillance

13.1 Purpose

The purpose of continuous monitoring and surveillance is to ensure that systems and components certified under this scheme continue to conform to requirements throughout the certification cycle and to identify nonconformities or risks that may arise after initial certification.

13.2 Certification Cycle

Certification is valid for a maximum period of **three years**, subject to successful surveillance and recertification audits.

Surveillance audits **shall be conducted annually** within ±30 days of the anniversary of the certification decision.

A recertification audit **shall be conducted** prior to the expiry of the three-year certification cycle.

13.3 Surveillance Audits

Surveillance audits **shall confirm**:

a) that the current practice statement is up to date and consistent with operations;
b) that scope boundaries and contexts of use remain unchanged or correctly updated;
c) that indicators of effectiveness are sustained;
d) that configuration management and change control processes are effective;
e) that privacy, security and acceptability obligations are being maintained;
f) that any corrective actions from the previous audit are closed.

Surveillance audits **shall sample** operational records, monitoring data and recent test evidence to confirm ongoing conformity.

Findings of surveillance audits **shall be documented** in a surveillance report, retained as part of the certification file.

Superseded

13.4 Continuous Monitoring

Clients **shall implement continuous monitoring** processes appropriate to their system or component under analysis.

Where technically feasible, continuous monitoring **shall include automated monitoring** of:

a) classification accuracy and error rates;
b) demographic outcome error parity;
c) resilience to attack vectors (e.g. replay or injection detection alerts);
d) security and privacy incidents;
e) operational performance (uptime, throughput, response times).

Continuous monitoring outputs **shall be reviewed** by the client and made available to the conformity assessment body at surveillance and recertification audits.

Continuous monitoring can also include connection to continuous use monitoring tools maintained by ACCS.

13.5 Intervening Audits and Notifications

Clients **shall notify** the conformity assessment body of any major change (Clause 4.8) or material incident affecting the system or component under analysis.

The conformity assessment body **shall determine** whether an intervening audit is required, which may be limited to the area affected by the change or incident.

Intervening audits may also be triggered by:

a) regulatory or supervisory findings;
b) substantiated complaints or adverse media;
c) withdrawal, suspension or expiry of external certifications relied upon (Clause 5.10).

13.6 Recertification Audits

Recertification audits **shall be conducted** prior to expiry of the three-year certification cycle.

Recertification audits **shall reassess** the system or component under analysis against the requirements of this scheme, including:

a) updated practice statement and governance records;
b) indicators of effectiveness using fresh test evidence;
c) any changes to scope, boundaries or contexts of use;
d) compliance with new or revised international and national requirements.

Where continuous monitoring evidence demonstrates sustained conformity, the conformity assessment body **may apply risk-based sampling** to reduce the scope of confirmatory testing at recertification.

Superseded

14. Future Alignment and Revision

This scheme has been developed in alignment with ISO/IEC 27566-1:2025 and informed by the emerging content of ISO/IEC 27566-3 (Committee Draft) together with IEEE 2089.1:2024.

The Scheme Owner shall monitor the development of further parts of ISO/IEC 27566 and related international standards.

Where new or revised international standards introduce requirements relevant to the certification of age assurance systems or components, the Scheme Owner shall:

a) review the scheme for consistency and completeness;
b) revise this document or associated annexes where necessary;
c) notify certified clients and UKAS of any transitional arrangements.

The conformity assessment body shall maintain procedures to ensure that certification decisions remain consistent with current international standards and recognised national requirements.

Revisions to this scheme shall be issued under controlled version management and shall state their relationship to previous editions and transitional requirements.

Annex A — Transition & Alignment from PAS 1296 and Legacy ACCS Standards

A.1 Purpose and use

This annex explains how ACCS 1:2025 consolidates and supersedes:

- PAS 1296:2018,
- ACCS 1:2020 (*Age Estimation Technologies*),
- ACCS 4:2020 (*Age Assurance Systems*),
- ACCS 1:2024 Addendum (Indicators of Effectiveness).Stake

It provides:

- A normative mapping of concepts and requirements,
- Clear statements of what is **unchanged**, **reframed**, **expanded** or **retired**,
- Practical **migration guidance** for certified clients,
- **Transitional arrangements** and timelines.

Note: Where ISO/IEC 27566-3 (in development) introduced new terminology or emphasis (e.g., "analysis/comparison"), ACCS 1:2025 uses compatible language while keeping ISO/IEC 27566-1 as the normative anchor.

Superseded

A.2 What changed at a glance

Area	PAS 1296 & Legacy ACCS	ACCS 1:2025 Alignment	Status
Foundation standard	PAS 1296 (UK)	ISO/IEC 27566-1 (global) + IEEE 2089.1 (online verification)	**Upgraded**
Scheme type	Product/service certification	ISO/IEC 17065 Type 6 scheme (system **or** component)	**Clarified**
Object of certification	"Service/System"	**System or component under analysis**; component-only allowed	**Expanded**
Indicators of effectiveness	ACCS Addendum (Basic–Strict)	Retained and harmonised with 27566-1 / IEEE 2089.1; demographic reporting	**Enhanced**
Testing approach	Ad hoc / fixed-sample tendencies	ISO/IEC/IEEE 29119 test design; reduced N with sequential/adaptive options; component & context testing	**Modernised**
Privacy/security	General principles	Explicit **attack vectors**, **binding**, **delivery integrity**, data minimisation; logs and deletion	**Strengthened**
Configuration mgmt	Minimal	ISO 10007-based; controls for RP dashboards to prevent efficacy "dial-down"	**New**

Continuous monitoring	Limited	Annual surveillance ±30 days; automated continuous monitoring "where feasible"	**New**
Interoperability	Limited	IEEE 2089.1 exchange options; optional IEEE certification/registry	**New/Optional**

A.3 Concept and terminology alignment

Concept	PAS 1296 / Legacy	ISO/IEC 27566 family	ACCS 1:2025 usage
The thing being certified	"Service/System"	"System/components"; Part 3 uses "analysis/comparison"	**System or component under analysis**
Methods	Verification/Estimation/Inference	Same + binding/successive validation emphasized	Same; plus, delivery/binding components
Effectiveness	Implied success/error	Indicators of effectiveness, demographic parity	**Basic/Effective/Highly Effective/Strict** with bounds
Evaluation term	"Evaluation/assessment"	Part 3 prefers "analysis/comparison"	**Analysis/comparison** (not "TOE")
Roles	Provider/Relying Party	Provider/RP/Intermediary clarified	Same, with detailed scoping (Clause 4)

Superseded

A.4 Requirement lineage tables

A.4.1 Scope, context and boundaries

PAS/Legacy ref.	Requirement (paraphrased)	ACCS 1:2025 clause	Change
PAS 1296 §4	Define scope and intended use	4.1–4.7	**Expanded** to component-only and contexts matrix
ACCS 4:2020 §5	Provide architecture overview	4.2(c), 4.6(a)	**Strengthened** (interfaces, dependencies)
—	Declare assumptions/exclusions	4.10	**New**
—	Data dependencies (authoritative vs non-authoritative)	4.9	**New**

A.4.2 Practice statements

PAS/Legacy ref.	Requirement	ACCS 1:2025 clause	Change
PAS 1296 §6	Document approach and controls	5.1–5.6	**Upgraded** to ISO/IEC 27566-1 Clause 10
—	Versioning, authority, records	5.8	**New**
—	Configuration management	5.7	**New (ISO 10007)**
—	Recognition of external evidence	5.9–5.10	**New**

A.4.3 Testing & indicators

PAS/Legacy ref.	Requirement	ACCS 1:2025 clause	Change
ACCS 1:2020 §7	Accuracy and performance testing	7.1–7.10; 8.2–8.6	**Generalised** via ISO 29119/25000/19795/30107
ACCS Addendum 2024	Levels Basic–Strict	10.3–10.8	**Retained** + demographic/CI bounds
—	Adaptive/sequential statistics	7.11–7.14	**New** (reduced N with rigour)

A.4.4 Privacy, security, acceptability

PAS/Legacy ref.	Requirement	ACCS 1:2025 clause	Change
PAS 1296 §7–§9	Privacy/security principles	6.5; 9.4(c–e); 4.5	**Strengthened** (attack vectors; delivery integrity; logs/deletion)
—	Accessibility/usability	9.4(e); 10.6	**Clarified** reporting & fairness

A.4.5 Lifecycle control

PAS/Legacy ref.	Requirement	ACCS 1:2025 clause	Change
PAS general	Maintain certification	13.2–13.6	**Expanded**: surveillance ±30 days, automated monitoring
—	Change control	4.8; 5.10	**New**: major/minor with intervening audits
ACCS 4:2020 §9	Certificates and scope listing	12.4–12.5	**Strengthened** (component/system, contexts, dependencies)

Superseded

A.5 Migration guidance for existing certificate holders

A.5.1 Who this applies to

- Clients certified under PAS 1296, ACCS 1:2020, ACCS 4:2020 and/or using the 2024 Addendum.

A.5.2 Minimum migration steps

1. **Re-scope (Clause 4):** Confirm system vs component under analysis, boundaries, contexts, assumptions/exclusions, data dependencies.
2. **Practice Statement upgrade (Clause 5):** Re-issue PS in 27566-1 structure; add configuration management (ISO 10007) and external evidence declarations.
3. **Test plan alignment (Clause 7):** Map legacy tests to ISO 29119 techniques; declare acceptance rules; consider reduced-N sequential designs.
4. **Indicators (Clause 10):** Translate any legacy accuracy claims into Basic/Effective/Highly Effective/Strict with CI/CrI bounds and demographic disclosure.
5. **Monitoring (Clause 13):** Implement automated monitoring where feasible; set up data capture for surveillance.
6. **Certificate/Schedule (Clause 12):** Ensure component vs system indicators and any local indicators are explicitly listed.

A.5.3 Timelines (default)

- **Within 6 months** of ACCS 1:2025 publication: complete re-scoping and updated practice statement.
- **At next surveillance** (annual ±30 days): adopt Clause 7/8/10 reporting formats.
- **By next recertification**: full migration complete.

Alternative transition plans may be approved case-by-case where justified.

Superseded

A.6 Equivalence, expansions and retirements

- **Equivalent** (direct carry-over): user eligibility outcomes; role definitions (provider/RP/intermediary); general privacy/security principles.
- **Expanded**: indicators of effectiveness (demographic parity and statistical bounds); component-only certification; configuration management; continuous monitoring; attack vector coverage (injection, deepfake, hill-climb, replay).
- **Retired/absorbed**: PAS 1296 UK-specific constructs where superseded by ISO/IEC 27566-1 global framing; duplicated legacy text now handled via cross-reference.

A.7 Optional interoperability and IEEE path

- ACCS 1:2025 supports optional **subsequent certification** to **IEEE 2089.1** and listing in the IEEE registry (Clause 12.6).
- Interoperability "shall" statements (e.g., exchanged checks, validity windows, non-replayable responses) are tested/audited where claimed, using Clauses 7–9 and reported in Clauses 10 & 12.

A.8 Governance and updates

- This Annex will be **maintained under controlled versioning**.
- When ISO/IEC 27566-3 (and further parts) are published, mappings will be added and clients notified in accordance with Clause 14 (Future Alignment and Revision).

A.9 Informative checklist (for auditors during transition)

- Scope boundary statement updated (4.6), incl. version/deployment/date
- Contexts of use matrix completed (4.7)
- Data dependencies declared (4.9)
- Assumptions/exclusions declared (4.10)
- Practice statement per 27566-1 Clause 10 (5.1–5.6); config mgmt (5.7); records (5.8)
- External evidence declared/weighted (5.9–5.10)
- Test plan per 29119, acceptance rules pre-registered (7.1–7.8, 7.11–7.14)
- Test reporting per 29119-3/19795-4/30107-3/25062 (8.4)
- Indicators table prepared (10.8), with demographic bounds (10.6)
- Continuous monitoring set up; KPIs defined (13.4)
- Certificate/Schedule drafts reflect component vs system indicators and limits (12.4)

Superseded

Annex B — Calculation of Audit Effort

B.1 Purpose and scope

This annex specifies the method for determining the audit effort required for certification, surveillance and recertification of systems or components under analysis. The approach is consistent with ISO/IEC 17065 (Type 6 scheme) and incorporates the framework set out in the *Calculation of Audit Effort* guidance document (informative reference).

Audit effort is determined on the basis of:

- the number and type of components included in scope,
- the declared contexts of use (Clause 4.7),
- the complexity and criticality of the system or component,
- national or jurisdictional requirements and
- indicators of effectiveness claimed (Clause 10).

B.2 Structure of audit effort

Audit effort is expressed in **auditor days** and comprises:

- **Stage 1 (Policy & Documentation Audit)**
- **Stage 2 (System/Component Audit)**
- **Evaluation Review**
- **Annual Surveillance Audits**
- **Recertification Audit**

Superseded

B.3 Base audit effort

- **Stage 1 Audit**: minimum **2 auditor days**, comprising review of the practice statement, governance, scoping, configuration management and readiness to proceed.
- **Stage 2 Audit**: minimum **4 auditor days** for a single-component system in one context of use.
- **Evaluation Review**: minimum **1 auditor day**.
- **Annual Surveillance Audit**: minimum **2 auditor days** per year.
- **Recertification Audit**: equivalent to initial Stage 2 effort, with adjustments for monitoring evidence (Clause 13).

B.4 Multipliers

The following multipliers are applied to Stage 2 and surveillance audit effort:

B.4.1 Component multiplier

- +1 day for each additional component under analysis beyond the first (e.g. verification + estimation).

B.4.2 Role multiplier

- +1 day if the client is acting in more than one role (e.g. provider + relying party).

B.4.3 Contexts of use multiplier

- +0.5 day for each additional sector (retail, gambling, social media, etc.) beyond the first.
- +0.5 day for each additional channel (online, offline, both).
- +1 day if results are reusable (persistent credentials).
- +1 day if global or multi-jurisdictional scope.

B.4.4 Criticality multiplier

- +1 day if the system is deployed in high-risk sectors (gambling, adult content, financial services).
- +1 day if the client claims "Highly Effective" or "Strict" indicators of effectiveness.

B.5 Reductions

Reductions in audit effort may be applied where credible external evidence exists, in accordance with Clause 5.9–5.10:

- Up to **25% reduction** where accredited ISO/IEC 27001 or 27701 certification is in place and in scope.
- Up to **25% reduction** where accredited biometric testing results (ISO/IEC 19795/30107) are submitted.
- Up to **10% reduction** where automated monitoring evidence demonstrates sustained conformity (Clause 13.4).

Total reductions shall not exceed **40% of base effort**.

B.6 Documentation

The conformity assessment body shall document the calculation of audit effort in the certification agreement, including:

- base audit effort,
- multipliers applied,
- reductions applied,
- total audit days allocated.

This calculation shall be recorded in the audit report (Clause 11.3) and reviewed at surveillance and recertification.

Superseded

B.7 Updates

The Scheme Owner shall periodically review this annex in light of operational experience, regulator expectations and updates to international standards.

Annex C — Practice Statement Template

C.1 Purpose

This annex provides a standardised template for practice statements required under Clause 5 of this scheme and ISO/IEC 27566-1, Clause 10. Clients are not obliged to use this exact format, but all practice statements **shall contain the elements listed here** to ensure comparability, auditability and completeness.

Superseded

C.2 Template structure

1. Administrative Information

- Legal entity name of client
- Registered address and jurisdiction(s) of incorporation
- Contact details for certification correspondence
- Version reference and date of issue of the practice statement
- Authorising officer (name, role, signature, approval date)

2. Scope of System or Component Under Analysis

- Name and version of system/component
- Deployment reference(s)
- Description of function(s) (verification, estimation, inference, binding, successive validation, delivery)
- Scope boundaries (inclusions/exclusions, dependencies)
- High-level architecture diagram

3. Contexts of Use (Clause 4.7)

- Sector(s) (e.g. retail, gambling, social media, regulated content, venues, others)
- Channel(s) (offline, online, both)
- Use type (single-use, reusable)
- Jurisdiction(s) of operation (national, regional, global)

4. Data Dependencies (Clause 4.9)

- List of data sources
- Classification as authoritative vs non-authoritative
- Primary vs secondary credentials
- Data access/validation dependencies
- Trust frameworks or contractual arrangements

5. Assumptions and Exclusions (Clause 4.10)

- Environmental assumptions (e.g. lighting, connectivity, device requirements)
- Demographic assumptions (e.g. dataset representativeness, coverage limits)
- Operational assumptions (e.g. human oversight, fallback)
- Exclusions (e.g. not suitable for <13s, not for offline use)

6. Functional, Performance, Privacy, Security, Acceptability Characteristics

For each characteristic (27566-1 Clause 5–9):

- Functional: suitability, completeness, correctness, appropriateness
- Performance: classification accuracy, throughput, scalability, response time
- Privacy: data minimisation, lawful basis, retention/deletion, subject rights
- Security: resilience to attack vectors (presentation, injection, replay, deepfake, hill-climb), secure delivery of results
- Acceptability: inclusivity, accessibility, usability, transparency, redress

7. Indicators of Effectiveness (Clause 10)

- Claimed indicator (Basic, Effective, Highly Effective, Strict)
- Evidence supporting the claim (test plan or external results)
- Demographic coverage and outcome error parity
- Confidence/credible bounds (where available)
- Local/jurisdictional indicators (if applicable)

8. Configuration Management (Clause 5.7)

- Who applies configuration settings (provider vs relying party)
- Safeguards against configurations that undermine conformity
- How updates and changes are controlled
- Access restrictions for configuration dashboards

9. Change Control and Records (Clause 5.8, 5.10)

- Authority responsible for approving and updating this statement

Superseded

- Version control history (changes, rationale, approval dates)
- Record-keeping arrangements (retention periods, archives)
- Process for notifying conformity assessment body of major changes or external certification lapses

10. External Certifications and Evidence (Clause 5.9)

- List of certifications held (e.g. ISO/IEC 27001, 27701, 30107 testing, others)
- Accreditation body (ILAC/IAF/EA member or other)
- Scope of certificate and relevance to this system/component
- Expiry date and surveillance cycle
- Weight placed on external evidence in this practice statement

11. Monitoring and Continuous Improvement

- Monitoring KPIs (classification accuracy, error parity, throughput, security events, privacy incidents)
- Automated monitoring processes (where feasible)
- Processes for internal review and continuous improvement
- Complaints and redress mechanism

Superseded

C.3 Guidance notes

- Practice statements **shall be public** (5.1), unless restricted by law; if restricted, an executive summary shall be public.
- Clients may use the free **ACCS Practice Statement Tool** (online) to generate structured outputs aligned with this annex.
- Practice statements **shall be updated annually** or on major changes.
- Practice statements **shall be consistent with the certificate and schedule** (Clause 12.4).

Annex D — Stage One Audit Report Template

D.1 Purpose

This template shall be used by auditors to record the outcome of the Stage One audit. Stage One audits confirm readiness to proceed to Stage Two by assessing practice statements, governance, scope and supporting documentation.

D.2 Template Structure

1. Administrative Information

- Client name and legal entity
- Registered address and jurisdiction(s)
- Contact person for audit
- Application reference number
- Date(s) of audit
- Audit location (on-site, remote, hybrid)
- Audit team members (lead auditor, technical experts, observers)
- Confirmation of impartiality and independence

2. Scope of Audit

- System or component under analysis (name, version, deployment reference)
- Declared role(s) (provider, relying party, intermediary)
- Scope boundaries (Clause 4.6)
- Contexts of use (Clause 4.7)
- Data dependencies (Clause 4.9)
- Assumptions and exclusions (Clause 4.10)
- National/jurisdictional obligations declared

3. Practice Statement Review

- Version and date of practice statement reviewed
- Confirmation that the PS contains all mandatory elements (Annex C)
- Cross-check of PS against:
  - Indicators of effectiveness declared (Clause 10)
  - Functional, performance, privacy, security, acceptability claims
  - External certifications or test results cited (Clause 5.9)
- Observed gaps or inconsistencies

4. Governance and Management Systems

- Authority for PS approval and change control (Clause 5.8)
- Record-keeping arrangements
- Configuration management policy (Clause 5.7)
- Monitoring and continuous improvement processes (Clause 13.4)

Superseded

- Management system certifications (e.g. ISO 9001, 27001, 27701, 42001) — with weight applied per Clause 5.9

5. Legal and Regulatory Checks

- Confirmation of legal entity status
- Disclosure of licences/registrations required in jurisdictions of operation
- Disclosure of any sanctions, enforcement actions or regulatory investigations
- Notes on potential jurisdictional constraints

6. External Evidence and Certifications

- List of certificates and external test reports reviewed
- Accreditation status of issuing bodies (ILAC/IAF/EA or other)
- Relevance to ISO/IEC 27566-1 requirements
- Weight applied (per Clause 5.9 categories 1–4)
- Notes on any required confirmatory testing

7. Risk and Threat Considerations

- Identification of threats and attack vectors declared (Clause 4.5)
- Assessment of whether PS adequately addresses risks (Clause 6.6)
- Observed gaps, exclusions or unjustified assumptions

8. Findings

- Conformities
- Nonconformities (major/minor)
- Observations and recommendations
- Determination of readiness to proceed to Stage Two

9. Audit Team Declarations

- Confirmation that audit was conducted in accordance with ACCS 1:2025 and ISO/IEC 17065 impartiality requirements
- Signatures of audit team leader and technical experts

10. Appendices (as applicable)

- Copy of practice statement reviewed
- Scope declaration and architecture diagram
- External certificates or reports submitted
- Change control/version history of PS
- Supporting policies (privacy, security, config management)

Superseded

Annex E — Stage Two Audit Report Template

E.1 Purpose

This annex provides the mandatory reporting template for Stage Two audits. Stage Two audits confirm, through direct evidence and observation, that systems or components under analysis conform to this scheme, ISO/IEC 27566-1 and other applicable standards. The completed Stage Two audit report forms part of the evaluation package for certification decision (Clause 12).

E.2 Template Structure

1. Administrative Information

- Client name and legal entity
- Registered address and jurisdiction(s)
- Contact person for audit
- Certificate application reference number
- Date(s) and duration of audit
- Audit location(s) (on-site, remote, hybrid)
- Audit team members (lead auditor, technical experts, observers)
- Confirmation of impartiality and independence

2. Scope of Audit

- System or component under analysis (name, version, deployment reference, release date)
- Roles audited (provider, relying party, intermediary)
- Scope boundaries (Clause 4.6)
- Contexts of use (Clause 4.7)
- Data dependencies (Clause 4.9)
- Assumptions and exclusions (Clause 4.10)
- National/jurisdictional requirements applied

3. Practice Statement Cross-Reference

- Version and date of practice statement reviewed
- Confirmation of PS completeness (Annex C checklist)
- Mapping table: **PS claim → evidence reviewed at Stage Two**

Superseded

- Notes on alignment, gaps or inconsistencies

4. Test Evidence Review

- Approved test plan(s) (Clause 7)
- Test execution and reporting (Clause 8)
- Summary of test results (classification accuracy, error rates, demographic coverage, performance metrics)
- Indicators of effectiveness achieved (Clause 10)
- Deviations from test plan and justification

5. Findings by Core Characteristic

For each characteristic, document conformity, evidence and nonconformities:

a) Functionality

- Suitability, completeness, correctness, appropriateness

b) Performance

- Accuracy levels (Basic/Effective/Highly Effective/Strict)
- Throughput, response times, scalability

c) Privacy

- Data minimisation, retention/deletion, rights management
- Logs reviewed, integrity protection, absence of prohibited biometric/ID data

d) Security

- Controls against attack vectors (presentation, injection, deepfake, hill-climb, replay)
- Secure delivery of results, replay prevention, fail-safe modes

e) Acceptability

- Usability, accessibility, inclusivity, transparency
- Complaints and redress handling

6. Component-Level Findings

- Findings for each component (verification, estimation, inference, binding, delivery, etc.)
- Indicators of effectiveness achieved per component
- System-level findings (integration outcomes)

7. Logs, Records and Monitoring Evidence

- Operational logs and audit trails reviewed
- Monitoring outputs (Clause 13.4)

Superseded

- Privacy/security incidents since last audit
- Complaints and redress records

8. National and Jurisdictional Requirements

- Summary of regulatory/sectoral requirements (e.g. gambling, content regulation, data protection)
- Evidence of compliance in declared jurisdictions
- Limitations or jurisdictional exclusions identified

9. Nonconformities and Corrective Actions

- List of nonconformities (major/minor)
- Associated clause references (ACCS 1:2025, ISO/IEC 27566-1, IEEE 2089.1)
- Corrective action plan agreed with client
- Timelines for remediation and verification

10. Audit Team Declarations

- Confirmation that audit was conducted in accordance with ACCS 1:2025 and ISO/IEC 17065 impartiality requirements
- Statement of independence and competence of team members
- Signatures of lead auditor and technical experts

11. Appendices

- Copy of practice statement reviewed
- Full test reports and raw data (where available)
- Architecture diagrams and scope declarations
- Change control and version records
- External certificates/test reports relied upon
- Monitoring dashboards and KPIs

Superseded

Annex F — Evaluation Review Template

F.1 Purpose

This template shall be used by evaluation reviewers to document their independent review of the Stage One and Stage Two audit packages. The evaluation review confirms that evidence is complete, consistent and sufficient to support the certification decision.

F.2 Template Structure

1. Administrative Information

- Client name and legal entity
- Certificate application reference number
- Reviewer name(s), role(s) and competence declaration
- Date of evaluation review
- Confirmation of independence from the audit and testing team

2. Review of Audit Package

- Stage One Audit Report received (Annex D) [Yes/No]
- Stage Two Audit Report received (Annex E) [Yes/No]
- Test reports and supporting evidence included [Yes/No]
- Practice statement (current version) included [Yes/No]
- Certificate and schedule draft included [Yes/No]

3. Completeness Check

- All mandatory clauses of ACCS 1:2025 addressed [Yes/No]
- All ISO/IEC 27566-1 “shall” requirements addressed [Yes/No]
- All IEEE 2089.1 “shall” requirements addressed [Yes/No]
- All contexts of use (Clause 4.7) covered [Yes/No]
- All indicators of effectiveness (Clause 10) reviewed [Yes/No]

4. Consistency Check

- Practice statement claims map to evidence in audit reports [Yes/No]
- Test results support declared indicators of effectiveness [Yes/No]
- Logs, monitoring and change control records align with scope [Yes/No]
- External certifications (Clause 5.9–5.10) valid and relevant [Yes/No]

5. Findings from Audit Reports

- Conformities confirmed [Yes/No]
- Nonconformities resolved or corrective action plan approved [Yes/No]
- Observations/limitations noted in certificate schedule [Yes/No]
- National/jurisdictional requirements confirmed [Yes/No]

6. Certificate and Schedule Draft Review

Superseded

- Certificate draft accurate and complete (Clause 12.4(b)) [Yes/No]
- Schedule draft includes:
  - scope boundaries and version reference
  - contexts of use
  - indicators of effectiveness (per component/system)
  - assumptions and exclusions
  - data dependencies
  - local/jurisdictional indicators
- Distinction between certified and non-certified elements clear [Yes/No]

7. Evaluation Reviewer Conclusions

- Evidence sufficient to support certification decision [Yes/No]
- Recommended decision:
  ☐ Grant certification
  ☐ Grant certification with conditions
  ☐ Defer certification (pending corrective actions)
  ☐ Refuse certification
- Summary of rationale (narrative text)

8. Reviewer Declarations

- I confirm that I am independent of the audit/testing team.
- I confirm that this review has been conducted in accordance with ACCS 1:2025 and ISO/IEC 17065 requirements.

Reviewer signature(s): _____
Date: _____

Superseded

Annex G — Model Certificate and Schedule of Certification

G.1 Purpose

This annex provides a model certificate and schedule of certification. Certification bodies shall use this model to issue certificates under this scheme. Minor formatting changes are permitted, but the required information shall not be omitted or altered.

G.2 Model Certificate

[Conformity assessment body Name & Logo]
Certificate of Conformity
Issued under the Age Check Certification Scheme (ACCS 1:2025)

Certificate No: [Unique number]
Issue Date: [DD/MM/YYYY]
Expiry Date: [DD/MM/YYYY]
Original Issue Date: [DD/MM/YYYY]
Client Name: [Legal entity name]
Registered Address: [Full address]

This is to certify that the system or component under analysis named below has been audited and found to conform with the requirements of **ACCS 1:2025 Technical Requirements for Age Assurance Systems**, in alignment with **ISO/IEC 27566-1** and **IEEE 2089.1**.

System/Component Certified:

- Name and version: [System/component name, version, deployment reference]
- Role(s): [Provider / Relying Party / Intermediary]

This certificate is valid only when read together with the accompanying Schedule of Certification.

Authorised by: _____
Name & Position: _____
Date: _____

Superseded

G.3 Model Schedule of Certification

[Conformity assessment body Name & Logo]
Schedule of Certification
Associated with Certificate No: [Unique number]

1. Scope of Certification

- System or Component under Analysis: [Name, version, deployment reference, release date]
- Scope boundaries: [Description of inclusions/exclusions, dependencies]
- Architecture summary: [High-level diagram reference if included]

2. Contexts of Use (Clause 4.7)

- Sector(s): [Retail, gambling, social media, etc.]
- Channel(s): [Offline, online, both]
- Use type: [Single-use, reusable]
- Jurisdiction(s): [National, regional, global]

3. Indicators of Effectiveness (Clause 10)

- Component-level indicators:
  - Verification: [Basic/Effective/Highly Effective/Strict]
  - Estimation: [Basic/Effective/Highly Effective/Strict]

    - Inference: [Basic/Effective/Highly Effective/Strict]
    - Binding / Delivery / Others: [Levels achieved]
- System-level indicator: [Overall level achieved]
- Demographic coverage: [Age bands, gender, skin tone, accessibility notes]
- Statistical confidence: [Confidence/credible bounds reported]

4. Assumptions and Exclusions (Clause 4.10)

- Environmental: [e.g. lighting, connectivity requirements]
- Demographic: [e.g. dataset limits, exclusions]
- Operational: [e.g. human oversight required]
- Explicit exclusions: [e.g. not for under-13s, not for offline use]

5. Data Dependencies (Clause 4.9)

- Authoritative data sources: [List]
- Non-authoritative/secondary sources: [List]
- Trust frameworks/contracts: [Summary]

6. National/Local Indicators (Clause 10.7)

- Additional jurisdictional indicators applied: [Details]

7. Monitoring and Surveillance

- Surveillance audit due dates: [Annual ±30 days]
- Recertification due date: [3 years from issue]

8. Limitations of Certification

- This certification applies only to the system or component under analysis as defined above.
- Any modifications outside the declared boundaries, contexts of use or configurations are **not certified**.
- Certification does not extend to relying party operations, data controllers or external systems not declared in scope.

Superseded

G.4 Public Registry Statement

For each certified client, the conformity assessment body shall publish a public registry entry including:

- Certificate number and validity dates
- Client name and jurisdiction
- Certified system/component name and version

- Scope summary
- Indicators of effectiveness achieved
- Contexts of use
- Any local indicators applied
- Status (active, suspended, withdrawn)

Annex H — Normative Mapping of "Shall" Requirements

H.1 Method and maintenance

- This annex is **normative for mapping** and **informative for notes**.
- When ISO/IEC 27566-3 (currently CD) is published, this annex will be updated under Clause 14 (Future Alignment and Revision).
- If a "shall" below is updated in a later edition of ISO/IEC 27566-1 or IEEE 2089.1, the scheme owner will issue a controlled revision to this annex and notify certified clients.

Superseded

H.2 ISO/IEC 27566-1 "Shall" requirements → ACCS 1:2025 clauses

H.2.1 Practice statements and governance (ISO/IEC 27566-1, Clause 10)

Requirement (paraphrased)	Coverage	ACCS 1:2025 Clause(s)	Notes
Provider shall publish/maintain a practice statement (PS) covering outcomes, methods, governance, indicators, logs and policies.	Both	5.1–5.6, 6.2(a), 11.3(b)	Annual review, public availability, auditor checks.
PS shall list components/methods (verification/estimation/inference/binding/successive validation).	Direct	5.2 (content), 4.2–4.4 (role-specific scope)	Component certification allowed.
PS shall declare data sources and whether authoritative/non-authoritative; primary/secondary credentials.	Direct	4.9, 5.2 (data sources)	Also on schedule: 12.4(c)(v).
PS shall declare indicators of effectiveness claimed and supporting evidence.	Direct	5.2, 10.2–10.8, 12.4.1	Reported per component/system.
Relying party PS shall state eligibility policy (age limits/bands), contexts, redress.	Both	4.7, 5.2, 6.2–6.3, 9.4(e)	Redress cross-ref ACCS 0.

Intermediary PS shall describe role/responsibilities and dependencies.	Direct	4.4, 5.2, 11.3(a)	Clear scope boundaries required.
PS shall be versioned, approved, controlled and retained.	Direct	5.8 (authority/records), 11.4(d)	Six-year retention (or 2 cycles).

H.2.2 Functional characteristics and operation

Requirement	Coverage	ACCS 1:2025 Clause(s)	Notes
System shall correctly interpret dates / avoid transposition errors.	Direct	5.2.3, 9.2(a), 9.4(a)	Checked Stage 2.
System shall bind result to the correct individual; prevent another's use.	Direct	4.5, 5.2, 7.4(b)(iv), 8.3(b)(iii), 9.4(d)	Includes PAD & replay controls.
Provider shall communicate standard configurations on request.	Direct	5.7(a,b), 6.2(e)	ISO 10007-based config mgmt.
Contexts of use shall be defined (sector/channel/use/jurisdiction).	Direct	4.7, 12.4.1	Drives audit effort.
Delivery shall maintain confidentiality/integrity of results.	Both	4.5, 7.4(b)(iv), 8.4(b)(v), 9.4(d)	Secure transport + anti-replay.

H.2.3 Performance and indicators

Requirement	Coverage	ACCS 1:2025 Clause(s)	Notes
Classification performance shall be measured, recorded and stated for each relevant configuration.	Direct	7.4–7.8, 8.3–8.4, 10.3–10.8	Includes reduced-N/statistical rigor.
Outcome error parity across demographics shall be addressed/disclosed.	Direct	7.5(c), 7.11–7.13, 10.6	Stratum lower bounds reported.
System shall be testable; scalability shall be evaluated.	Direct	7.4(b)(iii), 8.3(b)(ii), 9.4(b)	Performance efficiency in scope.

H.2.4 Privacy

Requirement	Coverage	ACCS 1:2025 Clause(s)	Notes
Collect/process only the minimum data necessary.	Direct	6.5(a), 9.4(c)	Data minimisation assessed.
Acquisition shall be solely for age-assurance result; onward use controlled.	Direct	6.5(b), 12.4.1	Reflected in schedule transparency.

Superseded

Access control and timely deletion shall be implemented; retain minimum logs.	Direct	6.5(b,c), 9.4(c), 13.4(b)(iv)	Logs sampled in Stage 2.
Relying party shall keep integrity-protected access logs; logs shall not contain biometric images/ID copies.	Direct	9.2(c), 9.4(c), 11.3(h)	Evidence in audit package.

H.2.5 Security (including attacks)

Requirement	Coverage	ACCS 1:2025 Clause(s)	Notes
System shall be resistant to presentation/injection/deepfake/replay/ hill-climb attacks.	Direct	4.5, 7.4(b)(iv), 8.3(b)(iii), 9.4(d)	Test methods chosen per 29119/30107/19795.
Results shall be protected against replay/forwarding/misuse; time-variant challenge.	Direct	4.5, 7.4(b)(iv), 8.4(b)(v), 9.4(d)	Delivery integrity requirements.
Failure modes shall be fail-safe (deny by default), logged, remediated.	Direct	9.2–9.4, 11.3(d), 13.5	Assessed during Stage 2.

H.2.6 Lifecycle, monitoring, change control

Requirement	Coverage	ACCS 1:2025 Clause(s)	Notes
Ongoing monitoring shall be maintained; major changes shall be notified.	Direct	4.8, 5.10, 13.3–13.6	±30-day surveillance; intervening audit triggers.
Version/scope boundaries shall be explicit on certificates/schedules.	Direct	4.6, 12.4.1, 11.3(a)	Architecture & boundary statement.

H.3 IEEE 2089.1 “Shall” requirements → ACCS 1:2025 clauses

(IEEE 2089.1 is referenced normatively in ACCS 1:2025; we align implementation and, where appropriate, treat these “shall” items as cross-referenced requirements tested/audited under Clauses 7–9.)

H.3.1 Interoperability and result exchange

Requirement (paraphrased)	Coverage	ACCS 1:2025 Clause(s)	Notes
Providers/Relying Parties shall not build a database of prior providers’ responses.	Direct	6.5(b), 9.4(c)	Privacy baseline + audit check.

Superseded

Checks shall be exportable/importable between compliant providers; requests shall redirect the user to original provider for re-authentication.	X-ref	7.4(b)(iv), 9.2(e), 12.6 (IEEE option)	Verified at Stage 2 where claimed.
Previous provider shall authenticate the user and return a standardised response in the same form; shall not include validation date in response.	X-ref	9.2(e), 9.4(d), 12.6	Delivery integrity & interoperability.
Exchanged checks shall have maximum validity periods tied to confidence level; both parties shall record volumes exchanged.	X-ref	10.3 (levels), 12.4.2 (schedule), 13.4(b)(i) (monitoring)	Logged and sampled in Stage 2/surveillance.

H.3.2 Outcomes, user rights and data handling

Requirement	Coverage	ACCS 1:2025 Clause(s)	Notes
Responses shall be yes/no (or minimal attribute) unless DOB strictly required.	X-ref	5.2 (claims), 9.4(c), 12.4(c)	Checked in PS and audit.
Personal data shall be deleted unless needed for reuse/legal obligation.	Direct	6.5(b), 9.4(c), 13.4(b)(iv)	Deletion controls and evidence sampled.
Users shall have a right to challenge/seek redress.	Direct	9.4(e); ACCS 0 cross-ref	Evidence of redress mechanism assessed.
Responses/results shall be integrity-protected and non-replayable.	Both	4.5, 7.4(b)(iv), 8.4(b)(v), 9.4(d)	Technical + process controls.

Superseded

H.4 Testing, reporting and indicators (cross-standard mapping)

Area	Coverage	ACCS 1:2025 Clause(s)	Notes
Test method selection shall follow recognised standards (ISO/IEC/IEEE 29119; ISO/IEC 25000; ISO/IEC 19795; ISO/IEC 30107; IEEE 2089.1 annexes).	Direct	7.1–7.4	Toolbox explicitly listed.
Test documentation/reporting shall meet international formats (29119-3; 19795-4; 30107-3; 25062).	Direct	8.4	Component/system results required.
Indicators shall be declared with statistical bounds; demographics disclosed; local indicators where applicable.	Direct	10.3–10.8	Reduced-N designs allowed with pre-registered rules (7.11–7.14).

H.5 Certificates, schedules and transparency

Requirement	Coverage	ACCS 1:2025 Clause(s)	Notes
Certificate/schedule shall enumerate scope boundaries, version/deployment, contexts, indicators (per component + system), data dependencies, assumptions/exclusions, local indicators/limits.	Direct	12.4.1	Public registry per 12.5; use of marks per ACCS 0.
Public disclosure shall provide indicator summaries and limitations (subject to lawful confidentiality).	Direct	10.2(d), 12.5(b), 11.3	Consistent with transparency rules.

H.6 Gaps and handling notes

- **Local/national requirements:** If a regulator mandates additional tests/thresholds, these are applied under **7.5 & 7.7** and **reported under 10.7**.
- **IEEE optional certification: 12.6** allows (but does not require) subsequent IEEE 2089.1 certification/registry listing; ACCS certification remains independent.
- **Future parts of ISO/IEC 27566:** See **Clause 14** for the controlled revision mechanism; Annex H will be updated accordingly.

H.7 Auditor use

Auditors should use this annex as a **checklist** during Stage 1 (readiness), Stage 2 (evidence review) and Evaluation Review, confirming that for each ISO/IEC 27566-1 and IEEE 2089.1 “shall” the corresponding ACCS 1:2025 clause was applied and evidenced in the audit package (Clause 11).

Superseded